有限亚Hamilton p群的分类

安立坚　著

北京工业大学出版社

前言

群论是近代数学的一个重要分支. 它是一门研究群的性质与结构的学科. 近年来, 随着科学技术的不断进步以及有限群论的逐步完善, 群论的思想、理论与方法已经渗透到科学领域的各个方面. 诸如在密码学、物理学、化学的分子结构等方面的应用就是明证, 而且群论的许多结果已被这些学科所吸收和利用.

在群论的众多分支中, 有限群论无论从理论本身还是从实际应用来说, 都占据着更为突出的地位. 同时, 它也是近年来比较活跃的一个数学分支, 有着十分丰富的内容. 在上个世纪, 经过很多数学家的努力, 在有限群中取得了一连串的突破, 并终于在 1981 年解决了著名的有限单群分类问题. 这项重大的科学成果的得来是很不容易的. 如果从 1832 年 Galois 证明交错群 A_5 是单群算起, 整整经历了 150 年. 参加这项工作的数学家前后共达几百人. 为了证明单群分类定理, 即有限单群共有 18 个无限族和 26 个零散单群, 人们使用了抽象群论的、表示论的 (包括常表示和模表示)、几何的以及组合论和图论的方法, 在杂志上发表了数千页以至上万页的证明. 直到 2005 年, D. Gorenstein, R. Lyons 和 R. M. Solomon 用六本专著才给出了单群分类定理的完整证明, 见文献 [26, 27, 28, 29, 30, 31] 等.

近年来, 随着有限单群分类的最终完成, 有限 p 群的研究才变得越来越活跃. 群论研究的许多领头科学家, 如 G. Glauberman, Z. Janko 等人开始转入对有限 p 群的研究, 发表了许多有限 p 群研究的论文, 见文献 [16, 23, 24, 25, 35, 36, 37, 38, 39, 40, 41, 42] 等.

在 p 群的研究领域中, 内交换 p 群和 Hamilton p 群的分类是两个经典的结果. 作为这两个经典结果的推广, 本书研究了子群或者交换或者正规的有限非交换 p 群, 我们称这类群为有限亚 Hamilton p 群. 本书给出了有限亚 Hamilton p 群的一些基本性质, 完成了有限亚

Hamilton p 群的完全分类, 并彻底解决了同构问题, 从而完整地解决了亚 Hamilton 群的分类问题. 为了方便读者, 我们对有限 p 群的一些基本结论和方法作了较详细的介绍. 本书还介绍了一些与亚 Hamilton p 群有关的工作.

安立坚

email: anlj@sxnu.edu.cn

2015 年 4 月于山西师范大学

目　录

第一章　基本概念和方法

本章介绍一些本书用到的基本结论和方法. 事实上, 这些结论和方法也是有限 p 群的研究中常常要用到的.

§1.1　基本概念和公式

本节首先给出有限 p 群的一些术语和符号, 其他未提及的术语和符号都是标准的, 见 [5, 7].

设 G 是有限 p 群, 我们分别用 $c = c(G)$、$d(G)$ 表示群 G 的幂零类、极小生成元的个数. G 的下中心群列和上中心群列分别是:

$$G = G_1 > G_2 > \cdots > G_{c+1} = 1,$$

和

$$1 = Z_0(G) < Z_1(G) < \cdots < Z_c(G) = G.$$

设 $\exp(G) = p^e$, 我们称 e 为群 G 的幂指数, 对于任意的 s, $0 \leqslant s \leqslant e$, 我们规定

$$\Lambda_s(G) = \{a \in G \mid a^{p^s} = 1\}, \quad V_s(G) = \{a^{p^s} \mid a \in G\},$$

并且规定

$$\Omega_s(G) = \langle \Lambda_s(G) \rangle, \quad \mho_s(G) = \langle V_s(G) \rangle,$$

则 G 的 Frattini 子群 $\Phi(G) = G'\mho_1(G)$.

下面我们重点来介绍证明和计算过程中反复使用的一些换位子公式.

命题 1.1.1. *设 G 是群, $a, b, c \in G$, 则*

(1) $a^b = a[a, b]$;

(2) $[a,b]^c=[a^c,b^c]$;

(3) $[a,b]^{-1}=[b,a]=[a,b^{-1}]^b=[a^{-1},b]^a$;

(4) $[ab,c]=[a,c]^b[b,c]=[a,c][a,c,b][b,c]$;

(5) $[a,bc]=[a,c][a,b]^c=[a,c][a,b][a,b,c]$;

(6) (*Witt*公式) $[a,b^{-1},c]^b[b,c^{-1},a]^c[c,a^{-1},b]^a=1$;

(7) $[a,b,c^a][c,a,b^c][b,c,a^b]=1$.

证明 (1)-(3) 由定义直接验证.

(4) $[ab,c]=(ab)^{-1}c^{-1}abc=(c^{-1})^{ab}c=(a^{-1}c^{-1}a)^bc^b(c^{-1})^bc=(a^{-1}c^{-1}ac)^b[b,c]=[a,c]^b[b,c]=[a,c][a,c,b][b,c]$.

(5) $[a,bc]=[bc,a]^{-1}=([b,a]^c[c,a])^{-1}=[a,c][a,b]^c=[a,c][a,b][a,b,c]$.

(6) 令 $u=aca^{-1}ba$. 轮换 a,b,c 三字母, 又令 $v=bab^{-1}cb$, $w=cbc^{-1}ac$. 则有

$$\begin{aligned}[a,b^{-1},c]^b &= b^{-1}[a,b^{-1}]^{-1}c^{-1}[a,b^{-1}]cb\\ &= b^{-1}ba^{-1}b^{-1}ac^{-1}a^{-1}bab^{-1}cb\\ &= (aca^{-1}ba)^{-1}(bab^{-1}cb)=u^{-1}v.\end{aligned}$$

同理有

$$[b,c^{-1},a]^c=v^{-1}w,\qquad [c,a^{-1},b]^a=w^{-1}u.$$

于是

$$[a,b^{-1},c]^b[b,c^{-1},a]^c[c,a^{-1},b]^a=u^{-1}vv^{-1}ww^{-1}u=1.$$

(7) 首先有

$$[a,b^{-1},c]^b=[[a,b^{-1}]^b,c^b]=[b,a,c^b].$$

同理又有

$$[b,c^{-1},a]^c=[c,b,a^c],\qquad [c,a^{-1},b]^a=[a,c,b^a],$$

于是由 Witt 公式有

$$[b,a,c^b][c,b,a^c][a,c,b^a]=1.$$

再互换 a,b 两个字母即得 (7) 式. □

若 G' 是交换群, 我们称 G 为亚交换群.

命题 1.1.2. 设 G 为亚交换群且 $x,y,z\in G$,

(1) 若 $z\in G'$, 则 $[z,x]^{-1}=[z^{-1},x]$;

(2) 若 $y\in G'$, 则 $[xy,z]=[x,z][y,z]$ 且 $[z,xy]=[z,x][z,y]$;

(3) $[x,y^{-1},z]^y=[y,x,z]$, $[x,y,z^x]=[x,y,z]$;

(4) $[x,y,z][y,z,x][z,x,y]=1$;

(5) 若 $z\in G'$, 则 $[z,y,x]=[z,x,y]$.

证明 (1) 由命题 1.1.1(3) 及 G' 的交换性得

$$[z,x]^{-1}=[z^{-1},x]^z=[z^{-1},x].$$

(2) 由命题 1.1.1(4–5) 及 G' 的交换性立得.

(3) 应用命题 1.1.1 中的诸换位子公式, 得

$$\begin{aligned}[x,y^{-1},z]^y &= [[x,y^{-1}]^y,z^y]=[[y,x],z[z,y]]\\ &= [y,x,z][[y,x],[z,y]]=[y,x,z].\end{aligned}$$

(4) 由 (3) 及 Witt 公式 (命题 1.1.1(6)) 立得.

(5) 由 $z\in G'$ 及 (4) 得

$$[y,z,x][z,x,y]=1,$$

即 $[z,x,y]=[y,z,x]^{-1}$. 由 (1), $[y,z,x]^{-1}=[[y,z]^{-1},x]=[z,y,x]$, 于是得 $[z,x,y]=[z,y,x]$. □

为了更好的叙述下面两个命题, 我们约定: 对于任意的正整数 i,j,

$$[ia,jb]=[a,b,\underbrace{a,\ldots,a}_{i-1},\underbrace{b,\ldots,b}_{j-1}].$$

命题 1.1.3. 设 G 为亚交换群, $a,b\in G$, m,n 为正整数, 则

$$[a^m,b^n]=\prod_{i=1}^{m}\prod_{j=1}^{n}[ia,jb]^{\binom{m}{i}\binom{n}{j}}.$$

证明 对 $m+n$ 用归纳法. 若 $m+n=2$, 公式显然成立. 下面设 $m+n>2$, 这时 m,n 中至少有一个大于 1.

若 $n>1$, 则

$$[a^m,b^n]=[a^m,b][a^m,b^{n-1}]^b.$$

据归纳假设得

$$\begin{aligned}[a^m,b^n] &= \prod_{i=1}^{m}[ia,b]^{\binom{m}{i}}\left(\prod_{i=1}^{m}\prod_{j=1}^{n-1}[ia,jb]^{\binom{m}{i}\binom{n-1}{j}}\right)^b\\ &= \prod_{i=1}^{m}[ia,b]^{\binom{m}{i}}\cdot\prod_{i=1}^{m}\prod_{j=1}^{n-1}([ia,jb][ia,(j+1)b])^{\binom{m}{i}\binom{n-1}{j}}\end{aligned}$$

$$\begin{aligned}&= \prod_{i=1}^{m}\left([ia,b]^{\binom{m}{i}}[ia,b]^{\binom{m}{i}\binom{n-1}{1}}[ia,nb]^{\binom{m}{i}}\right.\\ &\qquad\left.\cdot\prod_{j=2}^{n-1}[ia,jb]^{\binom{m}{i}\binom{n-1}{j}+\binom{m}{i}\binom{n-1}{j-1}}\right)\\ &= \prod_{i=1}^{m}\left([ia,b]^{\binom{m}{i}\binom{n}{1}}[ia,nb]^{\binom{m}{i}\binom{n}{n}}\prod_{j=2}^{n-1}[ia,jb]^{\binom{m}{i}\binom{n}{j}}\right)\\ &= \prod_{i=1}^{m}\prod_{j=1}^{n}[ia,jb]^{\binom{m}{i}\binom{n}{j}}.\end{aligned}$$

而若 $n=1$, 则 $m>1$. 这时有

$$[a^m,b]=[a^{m-1},b]^a[a,b].$$

应用归纳假设得

$$\begin{aligned}
[a^m, b] &= \left(\prod_{i=1}^{m-1}[ia,b]^{\binom{m-1}{i}}\right)^a [a,b] \\
&= \prod_{i=1}^{m-1}[ia,b]^{\binom{m-1}{i}} \prod_{i=1}^{m-1}[(i+1)a,b]^{\binom{m-1}{i}} \cdot [a,b] \\
&= [a,b][a,b]^{\binom{m-1}{1}} \prod_{i=2}^{m-1}[ia,b]^{\binom{m-1}{i}} \prod_{i=2}^{m}[ia,b]^{\binom{m-1}{i-1}} \\
&= [a,b]^{\binom{m}{1}} \left(\prod_{i=2}^{m-1}[ia,b]^{\binom{m}{i}}\right) [ma,b]^{\binom{m}{m}} \\
&= \prod_{i=1}^{m}[ia,b]^{\binom{m}{i}}.
\end{aligned}$$

□

命题 1.1.4. *设 G 为亚交换群, $a, b \in G$, $m \geqslant 2$, 则*

$$(ab^{-1})^m = a^m \prod_{i+j \leqslant m} [ia, jb]^{\binom{m}{i+j}} b^{-m}.$$

证明 用对 m 的归纳法. 当 $m = 2$ 时,

$$(ab^{-1})^2 = ab^{-1}ab^{-1} = a^2b^{-1}[b^{-1}, a]bb^{-2} = a^2[a,b]b^{-2},$$

结论成立. 现在设 $m > 2$, 由归纳假设有

$$\begin{aligned}
(ab^{-1})^m &= (ab^{-1})^{m-1}ab^{-1} \\
&= a^{m-1} \prod_{i+j \leqslant m-1} [ia, jb]^{\binom{m-1}{i+j}} b^{-m+1}ab^{-1} \\
&= a^{m-1} \prod_{i+j \leqslant m-1} [ia, jb]^{\binom{m-1}{i+j}} a[a, b^{m-1}]b^{-m} \\
&= a^m \prod_{i+j \leqslant m-1} [ia, jb]^{\binom{m-1}{i+j}} \\
&\quad \cdot \left(\prod_{i+j \leqslant m-1} [(i+1)a, jb]^{\binom{m-1}{i+j}}\right) [a, b^{m-1}]b^{-m}.
\end{aligned}$$

应用命题 1.1.3,

$$[a, b^{m-1}] = \prod_{j=1}^{m-1} [a, jb]^{\binom{m-1}{j}}.$$

代入上式得

$$\begin{aligned}
(ab^{-1})^m &= a^m \prod_{j=1}^{m-2} [a, jb]^{\binom{m-1}{j+1}} \prod_{\substack{i+j \leqslant m-1 \\ i>1}} [ia, jb]^{\binom{m-1}{i+j}} \\
&\quad \cdot \prod_{\substack{i+j \leqslant m \\ i>1}} [ia, jb]^{\binom{m-1}{i+j-1}} \prod_{j=1}^{m-1} [a, jb]^{\binom{m-1}{j}} b^{-m} \\
&= a^m \prod_{j=1}^{m-2} [a, jb]^{\binom{m}{j+1}} [a, (m-1)b] \prod_{\substack{i+j \leqslant m-1 \\ i>1}} [ia, jb]^{\binom{m}{i+j}} \\
&\quad \cdot \prod_{\substack{i+j = m \\ i>1}} [ia, jb] \cdot b^{-m} \\
&= a^m \prod_{j=1}^{m-1} [a, jb]^{\binom{m}{j+1}} \prod_{\substack{i+j \leqslant m \\ i>1}} [ia, jb]^{\binom{m}{i+j}} b^{-m} \\
&= a^m \prod_{i+j \leqslant m} [ia, jb]^{\binom{m}{i+j}} b^{-m}.
\end{aligned}$$

□

§1.2 Engel 条件

定义 1.2.1. 称群 G 满足 n **次** *Engel* **条件**, 如果对任意的 $g, h \in G$,

有

$$[g, \underbrace{h, \ldots, h}_{n}] = 1.$$

著名的 Zorn 定理断言, 满足 n 次 Engel 条件的有限群必为幂零群. 熟悉内幂零群的读者可以很容易地应用极小反例法证明这点. 这里就不证明了.

定理 1.2.2. 设群 G 满足 2 次 Engel 条件, 则 G 是幂零类至多为 3 的幂零群. 如果 G 中没有 3 阶元素, 则 $c(G) \leqslant 2$.

为证明这个定理, 先证明一个引理.

引理 1.2.3. 群 G 满足 2 次 Engel 条件当且仅当 G 中任意两个共轭元素可换.

证明 因为

$$[g, h, h] = [[g, h], h] = [h^{-g}h, h] = [h^{-g}, h]^h,$$

$[g, h, h] = 1$ 等价于 $[h^{-g}, h] = 1$, 即 h^g 与 h 可换. □

定理 1.2.2 的证明:

由引理 1.2.3, 任意元素 g 在 G 中的正规闭包 $A(g) := g^G = \langle g^x \mid x \in G \rangle$ 是 G 的交换正规子群.

我们分下列步骤来证明定理.

(1) 简单换位子 w 中有两项相等其值必为 1: 可设

$$w = [a_1, \ldots, a_s, x, b_1, \ldots, b_t, x, c_1, \ldots, c_u],$$

其中 s, t, u 均可以为 0. 即可以没有 $\{a_i\}$, $\{b_j\}$ 或 $\{a_k\}$. 于是

$$w_1 = [a_1, \ldots, a_s, x] \in A(x).$$

由 $A(x) \trianglelefteq G$, $w_2 = [w_1, b_1, \ldots, b_t] \in A(x)$. 再由 $A(x)$ 交换, $[w_2, x] = 1$, 从而 $w = 1$.

(2) 对任意的 $x, y \in G$, 有 $[x^{-1}, y] = [x, y^{-1}] = [x, y]^{-1}$: 由 $1 = [xx^{-1}, y] = [x, y]^{x^{-1}}[x^{-1}, y]$, 用 (1) 即得 $1 = [x, y][x^{-1}, y]$, $[x^{-1}, y] = [x, y]^{-1}$. 由此又得 $[x, y^{-1}] = [y^{-1}, x]^{-1} = [y, x] = [x, y]^{-1}$.

(3) Jakobi 恒等式成立: 对任意的 $x, y, z \in G$, 有 $[x, y, z][z, x, y][y, z, x] = 1$: 因为 $[x, y^{-1}, z] \in A(y)$, $[x, y^{-1}, z]^y = [x, y^{-1}, z]$. 再由 (2), $[x, y^{-1}, z] = [[x, y]^{-1}, z] = [x, y, z]^{-1}$. 由 Witt 恒等式得

$$[x, y, z]^{-1}[y, z, x]^{-1}[z, x, y]^{-1} = 1,$$

即 $[z, x, y][y, z, x][x, y, z] = 1$. 轮换 x, y, z 的位置, 即得所需结果.

(4) $[x, z, y] = [x, y, z]^{-1}$: 由 $[x, yz] = [x, z][x, y][x, y, z]$, 再用 (1) 得

$$[x, yz]^y = [x, z]^y[x, y]^y[x, y, z]^y = [x, z][x, z, y][x, y][x, y, z].$$

于是

$$\begin{aligned}[x, yz]^{yz} &= ([x, yz]^y)^z = [x, z]^z[x, z, y]^z[x, y]^z[x, y, z]^z \\ &= [x, z][x, z, y][x, y][x, y, z]^2.\end{aligned}$$

由 (1),

$$[x, yz]^{yz} = [x, yz] = [x, z][x, y][x, y, z].$$

因为上面两式右端的诸换位子都包含 x, 因此均属于 $A(x)$, 彼此交换. 由此二式相等, 得到 $[x, y, z][x, z, y] = 1$, 即 $[x, z, y] = [x, y, z]^{-1}$.

(5) $[x, y, z] = [y, x, z]^{-1}$: 由 (2), $[x, y, z] = [[y, x]^{-1}, z] = [y, x, z]^{-1}$, 得证.

由 (4) 和 (5) 说明, 任意交换 $[x, y, z]$ 中的两项, 其值变为原换位子的逆. 因此, 更一般地, 作 x, y, z 的奇置换, 其值变逆, 而作偶置换, 其值不变. 于是再应用 (3) 立得

(6) $[x,y,z]^3=1$.

至此, 如果 G 中没有 3 阶元素, 则 $[x,y,z]=1$, 即 G 是幂零类至多为 2 的幂零群.

(7) $[x,y,z,u]=[x,y,u,z]^{-1}$: 把 $[x,y]$ 作为一个整体, 应用 (4) 立得结论.

应用 (7), (6) 前面的那段话以及 (2), 对换位子 $[x,y,z,u]$, 作 x, y, z, u 的奇置换, 其值变逆, 而作偶置换, 其值不变. 细节从略.

(8) $[x,y,z,u]^2=1$: 由 $[x,y,z,u]=[[x,y],z,u]=[z,u,[x,y]]=[[z,u],[x,y]]=[[x,y],[z,u]]^{-1}=[x,y,[z,u]]^{-1}=[z,u,x,y]^{-1}=[x,y,z,u]^{-1}$, 得到结果.

把 $[x,y]$ 作为整体, 由 (6) 又得 $[x,y,z,u]^3=1$, 结合 (8) 即得到 $[x,y,z,u]=1$, 即 G 的幂零类至多为 3. □

§1.3 循环扩张理论

本节主要介绍循环扩张的基本理论. 所得结论不仅仅限于有限 p 群, 对有限群也是成立的.

定义 1.3.1. 称群 G 为**群 N 被群 F 的扩张**, 如果 N 是 G 的正规子群, 并且 $G/N\cong F$. 若 F 是一个 m 阶循环群, 则这时的扩张叫做**N 的 m 次循环扩张**. 若 $N\leqslant Z(G)$, 则这时的扩张叫做**中心扩张**.

设 G 是 N 的 m 次循环扩张. 因为 G/N 是 m 阶群, 所以有 $b^m\in N$, 其中 $G/N=\langle bN\rangle$. 又因为 $N\trianglelefteq G$, 所以 b 诱导出 N 的一个自同构 τ. 由于 $b^m\in N$, 存在 $a\in N$ 使得 $b^m=a$. 显然, $b^{-1}ab=a$. 所以我们有

$$a^\tau=a,\qquad \tau^m=\varphi(a). \tag{1.1}$$

其中 $\varphi(a)$ 表示由 a 诱导的 N 的内自同构. 反过来, 假定存在 $a\in N$ 和 $\tau\in\mathrm{Aut}(G)$ 满足 (1.1) 式, 则令 $G=\{(g^i,n)\mid 0\leqslant i\leqslant m-1, n\in N\}$

(只看成符号的集合). 如下规定 G 的乘法:

$$(g^i, n) \cdot (g^j, n') = \begin{cases} (g^{i+j}, n^{\tau^j} n'), & i+j < m, \\ (g^{i+j-m}, an^{\tau^j} n'), & i+j \geqslant m. \end{cases} \tag{1.2}$$

则 G 对上述乘法组成一个群, 有正规子群 $\overline{N} = \{(g^0, n) \mid n \in N\} \cong N$, 并且 $G/\overline{N} \cong \mathrm{C}_m$ (验证均从略). 我们把上面叙述的事实写成一个定理.

定理 1.3.2. 设 N 是群, $F = \langle g \rangle$ 是 m 阶循环群. 又设 $a \in N$, $\tau \in \mathrm{Aut}(N)$, a 与 τ 满足 (1.1) 式. 则集合 $G = \{(g^i, n) \mid 0 \leqslant i \leqslant m-1, n \in N\}$ 对于由 (1.2) 式定义的乘法组成一个群. G 是 N 被循环群 $F \cong \mathrm{C}_m$ 的扩张.

对于 N 是有限群的情形, 为了使用方便, 我们经常将定理 1.3.2 中的群 G 用生成元和定义关系组写出来. 即, 我们有下面的定理.

定理 1.3.3. 设 N 是有限群, $N = \langle n_1, n_2, \ldots, n_r \rangle$ 且

$$V = \{f_i(n_1, n_2, \ldots, n_r) = 1 \mid i \in I\}$$

为 N 的一个定义关系组. 若 $a \in N$, $\tau \in \mathrm{Aut}(N)$, a 与 τ 满足 (1.1) 式, 则 $G = \langle n_1, n_2, \ldots, n_r, b \rangle$ 是 N 的 m 次循环扩张, 其中 G 的定义关系组为:

$$V \cup \{b^{-1} n_i b = n_i^{\tau}, b^m = a \mid i \in I\}.$$

定理 1.3.2 给出了决定群 N 的所有循环扩张的方法. 但对于不同的 a, τ 确定的扩张何时同构的问题并没有回答. 下面的命题说明由与 τ 共轭的 N 的自同构 $\sigma^{-1}\tau\sigma$ 和元素 a^{σ} 得到的循环扩张与由 a, τ 确定的扩张是同构的.

命题 1.3.4. 如定理 1.3.2, 设 G 是 N 的 m 次循环扩张, 由满足 (1.1) 式的 $a \in N$ 和 $\tau \in \mathrm{Aut}(N)$ 得到. 再设 $\tau_1 = \sigma^{-1}\tau\sigma$ 是 $\mathrm{Aut}(N)$ 中与 τ 共轭的自同构. 则 $a_1 = a^{\sigma}$ 与 τ_1 满足 (1.1) 式, 并且由 a_1 和 τ_1 得到的 N 的 m 次循环扩张 G_1 与 G 同构.

证明 作为集合, 也有 $G_1 = \{(g^i, n) \mid 0 \leqslant i \leqslant m-1, n \in N\}$, 但其中乘法定义为

$$(g^i, n) \cdot (g^j, n') = \begin{cases} (g^{i+j}, n^{\tau_1^j} n'), & i+j < m, \\ (g^{i+j-m}, a_1 n^{\tau_1^j} n'), & i+j \geqslant m, \end{cases} \tag{1.3}$$

规定映射 $f: G \to G_1$: $(g^i, n) \mapsto (g^i, n^\sigma)$. 则 f 是 G 到 G_1 的同构. 只需验证 f 保持乘法运算. 因为对 $i+j<m$ 有

$$(g^i, n^\sigma) \cdot (g^j, n'^\sigma) = (g^{i+j}, n^{\sigma\tau_1^j} n'^\sigma) = (g^{i+j}, n^{\tau^j\sigma} n'^\sigma) = (g^{i+j}, (n^{\tau^j} n')^\sigma),$$

而对 $i+j \geqslant m$, 有

$$(g^i, n^\sigma) \cdot (g^j, n'^\sigma) = (g^{i+j-m}, a^\sigma n^{\sigma\tau_1^j} n'^\sigma) = (g^{i+j-m}, (a n^{\tau^j} n')^\sigma).$$

结合 (1.2) 式, 可以看出 f 保持运算. 证毕. □

循环群被循环群的扩张是特殊的循环扩张. 我们引入亚循环群的概念.

定义 1.3.5. 称 G 为**亚循环群**, 如果 G 有循环正规子群 N, 使商群 G/N 也是循环群. 即, 亚循环群为循环群被循环群的扩张.

下面的 Hölder 定理决定了有限亚循环群的构造.

定理 1.3.6. 设 $n, m \geqslant 2$ 为正整数, G 是 n 阶循环群 N 被 m 阶循环群 F 的扩张. 则 G 有如下定义关系:

$$G = \langle x, y \rangle,\ x^n = 1, y^m = x^t, y^{-1}xy = x^r, \tag{1.4}$$

其中参数 n, m, t, r 满足关系式

$$r^m \equiv 1 \pmod n,\ t(r-1) \equiv 0 \pmod n. \tag{1.5}$$

反之, 对每组满足 (1.5) 式的参数 n, m, t, r, (1.4) 式都确定一个 n 阶循环群被 m 阶循环群的扩张.

证明 设 G 是一个这样的扩张. $N = \langle x \rangle$, $x^n = 1$. 则存在 $a \in N$ 和 $\tau \in \mathrm{Aut}(G)$ 满足 (1.1) 式. 令

$$a = x^t, \qquad \tau : x \mapsto x^r.$$

由 $\tau^m = \varphi(a)$ 可得 $r^m \equiv 1 \pmod{n}$. 由 $x^\tau = x$ 可推出 $t(r-1) \equiv 0 \pmod{n}$. 故 (1.5) 式成立. 由定理 1.3.3 可得 G 的定义关系 (1.4) 式. □

下面举例说明如何利用循环扩张理论来解决比较简单的群的分类问题.

例 1.3.7. *决定所有的 8 阶群.*

解 首先, 由交换群分解定理, 8 阶交换群只有三种类型, 即 C_8, $C_4 \times C_2$ 和 $C_2 \times C_2 \times C_2$. 故以下可假定群 G 非交换. 如果 G 中所有非单位元都是 2 阶的, 则 G 是交换群. 于是 G 中存在 4 阶元. 又, 如果 G 有 8 阶元, 则 G 循环, 亦交换, 故 G 没有 8 阶元.

任取 G 的一个 4 阶元 a. 它生成的子群 A 是 G 的极大子群, 所以 $A \trianglelefteq G$, 且商群 G/A 是 2 阶循环群, 于是 G 是亚循环群. 由定理 1.3.6,

$$G = \langle a, b \mid a^4 = 1, b^2 = x^t, b^{-1}ab = a^r \rangle$$

其中参数 t, r 满足关系式

$$r^2 \equiv 1 \pmod{4}, \ t(r-1) \equiv 0 \pmod{4}. \tag{1.6}$$

因为我们只考虑非交换群, 所以 $r = -1$. 由 (1.6) 可得 $2 \mid t$. 当 $t = 0$ 时, G 有定义关系:

$$G = \langle a, b \mid a^4 = b^2 = 1, b^{-1}ab = a^{-1} \rangle.$$

这时 G 是 8 阶二面体群. 当 $t = 2$ 时, G 有定义关系:

$$G = \langle a, b \mid a^4 = 1, b^2 = a^2, b^{-1}ab = a^{-1} \rangle.$$

这时 G 是 8 阶四元数群. □

§1.4 有限 p 群的循环扩张

由定理 1.3.2 和 1.3.4 可知, N 循环扩张需要考虑 N 的自同构群的共轭类. 但是在实际中, 我们做循环扩张时往往是从确定定理 1.3.3 中的定义关系入手. 对于有限 p 群的循环扩张尤其是这样. 由定理 1.3.3 可知, 要确定 N 的 m 次循环扩张 $G = \langle N, b\rangle$, 只需要确定 $b^{-1}n_ib$ 和 b^m 的值, 其中 $N = \langle n_1, n_2, \ldots, n_r\rangle$. 而确定 $b^{-1}n_ib$ 的值等价于确定 $[n_i, b] = n_ib^{-1}n_ib$ 的值. 在进行有限 p 群的循环扩张时, 下面的简单的定理发挥着重要的作用, 可以有效地帮助我们判断 $[n_i, b]$ 的取值范围.

定理 1.4.1. 设 G 是有限 p 群, M 和 N 都是 G 的正规子群且 $|M : N| = p$. 则对于任意的 $g \in G$ 和 $m \in M$, 有 $[m, g] \in N$.

证明 由对应定理可知 M/N 是 G/N 的 p 阶正规子群. 从而 $M/N \leqslant Z(G/N)$. 故对于任意的 $g \in G$ 和 $m \in M$ 有 $[mN, gN] = N$. 所以 $[m, g] \in N$. □

若 G 是 N 的循环扩张, 则 N 的特征子群一定是 G 的正规子群. 在进行有限 p 群的循环扩张时, 我们应当尽可能多地寻找到 N 的特征子群. 这样就可以尽量多地应用定理 1.4.1 来确定所需换位子的取值范围. 以下我们举例说明.

例 1.4.2. 设 G 是 $\mathcal{D}_8$ 的 2 次循环扩张. 则 G 是下列群之一:

(1) 二面体群: $G = \langle a, b \mid a^8 = 1,\ b^2 = 1,\ [a, b] = a^{-2}\rangle$.

(2) 半二面体群: $G = \langle a, b \mid a^8 = 1,\ b^2 = 1,\ [a, b] = a^2\rangle$.

(3) $G \cong \mathcal{D}_8 \times \mathrm{C}_2$.

(4) $G = \langle a, b, c \mid a^4 = b^2 = c^2 = 1, [a, b] = a^2, [a, c] = [b, c] = 1\rangle, (\cong \mathcal{D}_8 * \mathrm{C}_4 \cong \mathrm{Q}_8 * \mathrm{C}_4)$.

解 设 $G = \langle N, x\rangle$ 是 N 的 2 次循环扩张, 其中 $N = \langle a, b \mid a^4 = b^2 = 1, [a, b] = a^2\rangle \cong D_8$. 由于 $N' = \langle a^2\rangle$ char N, $N' \trianglelefteq G$. 由于 $A = \langle a\rangle$

是 N 的唯一的循环极大子群, 所以 A char N. 进一步也有 $A \trianglelefteq G$. 现在我们得到一个 G 的主群列:

$$G > N > A > N' > 1.$$

由定理 1.4.1, 我们有 $[b, x] \in A$, $[a, x] \in N'$ 和 $[a^2, x] = 1$. 从而我们可以设

$$[a, x] = a^{2i}, \quad [b, x] = a^j.$$

计算可得 $[a, x^2] = [a, x]^2[a, x, x] = 1$, 所以可设 $x^2 = a^k$.

若 $[a, x] = a^2$, 则 $[a, xb] = 1$. 所以我们可不妨设 $[a, x] = 1$ (必要时用 xb 来替换 x, 为什么?). 此时, 我们可用两种方法来计算 $[b, x^2]$. 一是:

$$[b, x^2] = [b, x]^2[b, x, x] = a^{2j}. \tag{1.7}$$

另一种方法是:

$$[b, x^2] = [b, a^k] = a^{2k}. \tag{1.8}$$

由 (1.7) 和 (1.8) 式可得 $j \equiv k \pmod 2$.

若 j, k 均为奇数, 我们可不妨设 $x^2 = a$(若 $x^2 = a^3$, 则用 xa 去替换 x 或者用 a^3 代替 a). 此时, 若 $[b, x] = a$, 则

$$G = \langle x, b \mid x^8 = b^2 = 1, [x, b] = x^{-2} \rangle.$$

G 是本定理中的 (1) 型群. 若 $[b, x] = a^3$, 则

$$G = \langle x, b \mid x^8 = b^2 = 1, [x, b] = x^2 \rangle.$$

G 是本定理中的 (2) 型群.

若 j, k 均为偶数, 我们可不妨设 $[b, x] = 1$(若 $[b, x] = a^2$, 则用 xa 去替换 x). 此时, 若 $x^2 = 1$, 则 $G = \langle a, b \rangle \times \langle x \rangle$ 是本定理中的 (3) 型群. 若 $x^2 = a^2$, 则 $G = \langle a, b \rangle * \langle x \rangle$. G 是本定理中的 (4) 型群. □

§1.5 有限 p 群的中心扩张

本节我们介绍利用中心扩张来构造有限 p 群的方法. 由于 p 群的中心非平凡, 所以中心扩张在有限 p 群的研究中是常见的并且重要的. 由中心扩张的定义, 下面的定理是显然的.

定理 1.5.1. 设 G, N, F 是群, 其中

$$N = \langle n_1, n_2, \ldots, n_s \mid n_j^{\alpha_j} = 1,\ [n_j, n_k] = 1,\ 1 \leqslant j \leqslant s,\ 1 \leqslant j < k \leqslant s\rangle,$$

$$F = \langle x_1, x_2, \ldots, x_r \mid f_i(x_1, x_2, \ldots, x_r) = 1,\ 1 \leqslant i \leqslant m\rangle.$$

若存在 $N_1 \leqslant Z(G)$ 使得 $N_1 \cong N$ 且 $G/N_1 \cong F$, 则存在数组 β_{ij}, 其中 $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant s$, $1 \leqslant \beta_{ij} \leqslant \alpha_j$, 使得

$$G = G(\beta_{ij}) = \langle a_1, a_2, \ldots, a_r, b_1, b_2, \ldots, b_s\rangle$$

具有以下定义关系:

$$f_i(a_1, a_2, \ldots, a_r) = b_1^{\beta_{i1}} b_2^{\beta_{i2}} \ldots b_s^{\beta_{is}}, \quad 1 \leqslant i \leqslant m,$$

$$b_j^{\alpha_j} = 1,\ [b_j, b_k] = 1, \quad 1 \leqslant j \leqslant s,\ 1 \leqslant j < k \leqslant s,$$

$$[a_l, b_j] = 1, \quad 1 \leqslant j \leqslant s,\ 1 \leqslant l \leqslant r.$$

其中 $N_1 = \langle b_1, b_2, \ldots, b_s\rangle$.

定理1.5.1的逆是不对的. 任意给定一个数组 β_{ij}, 定理中 N_1 不一定与 N 同构. 例如, 当 $F = \langle x_1, x_2\rangle \cong Q_8$ 且 $N = \langle n\rangle \cong C_2$ 时, 令 $G = \langle a_1, a_2, n\rangle$ 满足如下定义关系组:

$$n^2 = 1, [n, a_1] = [n, a_2] = 1, a_1^4 = n, a_2^2 = a_1^2, [a_1, a_2] = a_1^2.$$

则 G 仍然与 Q_8 同构.

下面我们仍然是用例子来说明中心扩张的方法.

例 1.5.2. 决定所有的 p^3 阶群, 其中 p 为奇素数.

解 首先, 由交换群分解定理, p^3 阶交换群只有三种类型, 即 C_{p^3}, $C_{p^2}\times C_p$ 和 $C_p\times C_p\times C_p$. 故以下可假定该群 G 非交换.

任取 p 阶正规子群 N, 则因 $|G/N|=p^2$, G/N 是交换群, 得 $N\geqslant G'$. 但 $G'\neq 1$, 则必有 $N=G'$, 并且 $G'\leqslant Z(G)$. 若 G/N 循环, 可设 $G/N=\langle aN\rangle$. 此时 $G=\langle a,N\rangle=\langle a\rangle$ 与 G 非交换矛盾. 从而 G/N 为 p^2 阶初等交换群. 设 $G/N=\langle aN,bN\rangle$, 则 $a^pN=N$ 且 $b^pN=N$. 再设 $N=\langle x\rangle$, 则 $G=\langle a,b\rangle$ 满足以下关系

$$x^p=1, a^p=x^i, b^p=x^j, [a,b]=x^k, [x,a]=[x,b]=1.$$

由于 G 非交换, 所以 $(k,p)=1$. 通过适当的替换, 我们可不妨设 $[a,b]=x$.

以下我们可分为两种情形.

情形一: G 中有 p^2 阶元素, 即 $(i,p)=1$ 或 $(j,p)=1$.

此时我们不妨设 $(i,p)=1$. 用 b^i 去替换 b 我们可得 $[a,b]=a^p$ 和 $b^p=a^{jp}$. 再用 ba^{-j} 去替换 b 可得:

$$G=\langle a,b \mid a^{p^2}=b^p=1, [a,b]=a^p\rangle. \tag{1.9}$$

情形二: G 中无 p^2 阶元素, 即 $i\mid p$ 且 $j\mid p$. 此时

$$G=\langle a,b \mid a^p=b^p=x^p=1, [a,b]=x, [x,a]=[x,b]=1\rangle. \tag{1.10}$$

下面我们验证由 (1.9) 式和1.10式给出的群确实是 p^3 阶群. 在 (1.9) 式中, 取 $N=\langle a \mid a^{p^2}=1\rangle$ 和 $\tau: a\mapsto a^{1+p}$. 则 $\tau^p=\varphi(1)$. 由定理 1.3.3 可知, G 是 N 的 p 次循环扩张. 从而 G 为 p^3 阶群.

在 (1.10) 式中, 取 $N=\langle a,x \mid a^p=x^p=1, [a,x]=1\rangle$ 和 $\tau: a\mapsto ax, x\mapsto x$. 则 $\tau^p=\varphi(1)$. 由定理 1.3.3 可知, G 是 N 的 p 次循环扩张. 从而 G 为 p^3 阶群.

由于这两个群的方次数不同, 所以它们显然是互不同构的. □

注 1.5.3. 在例 1.5.2 中, (1.10) 式中保留了关系 $[x,a]=[x,b]=1$. 而 (1.9) 式中则去掉了关系 $[a^p,b]=1$. 这说明中心扩张时最终也需要利用循环扩张理论来判断最终的结果是否正确. 但是, 中心扩张确实可以起到简化运算的作用.

第二章　内交换 p 群和 Dedekind p 群

§2.1　内交换 p 群

一个非交换群称为**内交换群**, 若它的每个真子群是交换的. 作为这个概念的延伸, 一个非交换 p 群称为 $\mathcal{A}_t$**群**, 若它至少有一个指数为 p^{t-1} 的非交换子群, 但它的所有指数为 p^t 的子群都交换. 显然, 内交换 p 群恰是 $\mathcal{A}_1$ 群. 内交换群可看做交换性最好且应是结构最简单的非交换群.

引理 2.1.1. *设 G 是有限非交换 p 群. 则 G 的交换极大子群的个数为 $0,1$ 或 $1+p$.*

证明　设 G 至少有两个不同的交换极大子群. 下证 G 的交换极大子群的个数是 $1+p$.

设 M_1 和 M_2 是 G 的两个不同的交换极大子群. 由此可得 $G = M_1M_2$, $Z(G) \leqslant M_1$ 且 $Z(G) \leqslant M_2$, $M_1 \cap M_2 \leqslant Z(G)$. 于是 $Z(G) = M_1 \cap M_2$. 因为 $G/M_1 \cong M_2/M_1 \cap M_2 = M_2/Z(G)$, 故 $|G : Z(G)| = p^2$. 因为 G 非交换, 故 $\overline{G} = G/Z(G) \cong C_p \times C_p$. 在此情形下可以证明: $\overline{M}$ 是 $\overline{G}$ 的极大子群当且仅当 M 是 G 的交换极大子群. (事实上, 因为 G 的交换极大子群都包含中心, 由对应定理可知, G 的极大子群个数与 $G/Z(G)$ 的极大子群个数相同. 又 $|M : Z(G)| = p$, 故 M 交换) 容易看出, $\overline{G}$ 有 $1+p$ 个极大子群. 因此 G 的交换极大子群的个数是 $1+p$.□

引理 2.1.2. *若有限 p 群 G 有非交换极大子群, 则 G 的非交换极大子群个数至少为 p.*

证明　设 G 是 d 元生成的. 则 $d(G) \geqslant 2$ 且 $|G/\Phi(G)| = p^d$. 故 $G/\Phi(G)$ 可看成 $GF(p)$ 上 d 维向量空间. G 的极大子群的个数即为 $G/\Phi(G)$ 的 $d-1$ 维子空间的个数. 容易计算 $d-1$ 维子空间的个数为

$\frac{p^d-1}{p-1}=1+p+p^2+\cdots+p^{d-1}$. 因为 G 非交换, 所以 G 的极大子群的个数至少是 $1+p$. 由引理 2.1.1 即得. □

下面我们准备分类内交换 p 群. 先介绍两个定理. 它们本身具有独立的意义.

第一个定理由段学复先生 1950 年在 [60] 中给出. 它在有限 p 群研究中经常用到.

定理 2.1.3. 设有限非交换 p 群 G 有交换极大子群. 则

$$|G|=p|G'||Z(G)|.$$

证明 设 A 是 G 的交换极大子群. 则 $A\lhd G$. 令 $g\in G\setminus A$. $\phi: A\longrightarrow A$ 是一个映射, 其定义为: $\phi(a)=[a,g]$. 若 $a,b\in A$, 则

$$\phi(ab)=[ab,g]=[ag,b]^b[b,g]=[a,g][b,g]=\phi(a)\phi(b).$$

故 ϕ 是同态. 又 $G=\langle g,A\rangle$ 是非交换的, 则

$$\mathrm{Ker}(\phi)=\{a\in A\mid [a,g]=1\}=C_A(G)=Z(G).$$

令 $K=\mathrm{Im}(\phi)$. 则 $K\leqslant G'<A$. 因为 A 是交换的且 $[a,g]^g=[a^g,g]\in K\cap A$, 故 $K\lhd G$. 又 $a^g=a[a,g]\in aK$, 故 g 中心化 A/K. 从而 G/K 交换且 $K=G'$. 又 $A/\mathrm{Ker}(\phi)\cong\mathrm{Im}(\phi)$, 我们有 $|G|=p|A|=p|\mathrm{Ker}(\phi)||\mathrm{Im}(\phi)|=p|Z(G)||G'|$. □

第二个定理由陈重穆先生 1985 年在 [1] 中给出. 它给出一个 p 群是内交换的等价条件, 在本书中经常用到.

定理 2.1.4. 设 G 是有限 p 群, 则下列命题等价:

(1) G 是内交换群;

(2) $d(G)=2$ 且 $|G'|=p$;

(3) $d(G)=2$ 且 $Z(G)=\Phi(G)$.

证明 (1) $\Rightarrow$ (2): 取二元素 $a, b \in G$ 使 $[a, b] \neq 1$. 则 $H = \langle a, b\rangle$ 非交换, 并因而 $H = G$. 因此 $d(G) = 2$. 取 G 的两个不同的极大子群 A 和 B. 由假设它们交换. 又由 A, B 的极大性得 $G = AB$. 因此 $A \cap B = Z(G)$. 再由同构定理, $AB/A \cong B/A\cap B$. 从而 $|G : A\cap B| = p^2$. 由定理 2.1.3, $|G| = p|G'||Z(G)|$, 于是 $|G'| = p$, (2) 成立.

(2) $\Rightarrow$ (3): 因为 $|G'| = p$, 有 $G' \leqslant Z(G)$. 则 G 为类 2 群. 计算可得 $[x^p, y] = [x, y]^p = 1$, 其中 $x, y \in G$. 于是 $\mho_1(G) \leqslant Z(G)$. 因此又有 $\Phi(G) = \mho_1(G)G' \leqslant Z(G)$. 如果 $\Phi(G) < Z(G)$, 则由 $d(G) = 2$ 推出 $|G/Z(G)| \leqslant p$, 于是 G 交换, 矛盾. 故 (3) 成立.

(3) $\Rightarrow$ (1): 因为每个极大子群 $M \geqslant \Phi(G) = Z(G)$, 且 $d(G) = 2$, 故 M 交换, 即 (1) 成立. □

p^3 阶非交换群是阶最小的内交换 p 群. 第一章我们已经给出了它的分类. 现在我们将其重述如下.

定理 2.1.5. *设 G 是 p^3 阶非交换群. 则 G 是下列互不同构的群之一:*

(1) $p = 2$.

(I) $\langle a, b \mid a^4 = b^2 = 1, b^{-1}ab = a^3\rangle \cong D_8 \cong \mathrm{M}_2(2,1) \cong \mathrm{M}_2(1,1,1)$;

(II) $\langle a, b \mid a^4 = 1, b^2 = a^2, b^{-1}ab = a^3\rangle \cong Q_8$.

(2) $p \neq 2$.

(I) $\langle a, b \mid a^{p^2} = b^p = 1, b^{-1}ab = a^{1+p}\rangle \cong \mathrm{M}_p(2,1)$;

(II$'$) $\langle a, b, c \mid a^p = b^p = c^p = 1, [a, b] = c, \quad [a, c] = [b, c] = 1\rangle \cong \mathrm{M}_p(1,1,1)$.

下面是 Rédei 于 1947 年在 [54] 中给出的内交换 p 群的分类. 这里给出的证明完全不同于 Rédei 的原始证明.

定理 2.1.6. G 是内交换 p 群当且仅当 G 是下列互不同构的群之一. 但有一个例外, 即有参数 $p=2$, $m=1$, $n=2$ 的 (ii) 型群和有参数 $p=2$, $m=n=1$ 的 (iii) 型群同构, 它们都给出 8 阶二面体群 D_8.

(i) Q_8;

(ii) $\mathrm{M}_{n,m,p} := \langle a, b \mid a^{p^n} = b^{p^m} = 1, a^b = a^{1+p^{n-1}} \rangle$, $n \geqslant 2$, $m \geqslant 1$, (亚循环);

(iii) $\mathrm{N}_p(n, m, p) := \langle a, b, c \mid a^{p^n} = b^{p^m} = c^p = 1, [a, b] = c, [c, a] = [c, b] = 1 \rangle$, $n \geqslant m \geqslant 1$, (非亚循环情形).

证明 $\Longleftarrow$: 对于群 (i), 由 p^2 阶群均交换即得. 对于群 (ii), 令 $\overline{G} = G/\langle a^{p^{n-1}} \rangle$. 则 $\bar{a}^{\bar{b}} = \bar{a}$. 即 $\overline{G}$ 是交换的. 故 $G' \leqslant \langle a^{p^{n-1}} \rangle$. 对于群 (iii), 令 $\overline{G} = G/\langle c \rangle$. 类似可证, $G' \leqslant \langle c \rangle$. 在任何情形下, 由于 $G' \neq 1$ 即得 $|G'| = p$. 又 $d(G) = 2$. 由定理 2.1.4 即得结论.

$\Longrightarrow$: p^3 阶非交换群均为内交换群, 它们是 Q_8, $\mathrm{D}_8 \cong \mathrm{M}_2(2,1) \cong \mathrm{M}_2(1,1,1)$ (对 $p=2$), 以及 $\mathrm{M}_p(2,1)$, $\mathrm{M}_p(1,1,1)$ (对 $p>2$). 故下面可设 $|G| > p^3$. 由定理 2.1.4, $d(G) = 2$, $|G'| = p$. 取 $a, b \in G$ 使得 $[a, b] \neq 1$ 且 $\bar{a} = aG', \bar{b} = bG'$ 是 $\overline{G} = G/G'$ 的基, 即 $\overline{G} = \langle \bar{a} \rangle \times \langle \bar{b} \rangle$, 并且使 $o(a)o(b)$ 最小. 设 $o(a) = p^n$, $o(b) = p^m$ 且 $n \geqslant m$.

我们首先断言: $\langle a \rangle \cap \langle b \rangle = 1$.

若否, 因为 $\bar{a} \cap \bar{b} = \bar{1}$, 也即 $\overline{\langle a \rangle \cap \langle b \rangle} = \bar{1}$. (此结论在 $G/G' = \overline{G} = \langle \bar{a} \rangle \times \langle \bar{b} \rangle$ 的条件下成立. 一般不对!) 从而 $1 \neq \langle a \rangle \cap \langle b \rangle \leqslant G'$. 则 $\langle a \rangle \cap \langle b \rangle = G'$. 设 $G' = \langle d \rangle$. 则 $o(d) = p$. 进一步可设 $d = a^s = b^t$. 则 $d^p = a^{sp} = b^{tp} = 1$. 于是 $p^n \mid sp$, $p^m \mid tp$. 设 $s = p^{n-1}s_1$, $t = p^{m-1}t_1$. 因为 $o(d) = p$, 故 $(s, p) = (t, p) = 1$. 从而 $(s_1, p) = (t_1, p) = 1$. 令 $a_1 = a^{s_1}, b_1 = b^{t_1}$. 则 $d = a_1^{p^{n-1}}$, $d = b_1^{p^{m-1}}$. 不失普遍性可设 $a^{p^{n-1}} = d$, $b^{p^{m-1}} = d$. 于是 $a^{p^{n-1}} = b^{p^{m-1}}$. (注意: 要保证 a_1, b_1 仍然满足 a, b 的条件!)

因为 $G' \leqslant Z(G)$, 故 G 是类 2 的. 从而对任意的 $x, y \in G$, 有

$$\begin{cases} (xy)^p = x^p y^p, & p > 2 \\ (xy)^2 = x^2 y^2 [y, x], & p = 2. \end{cases} \tag{2.1}$$

若 $p > 2$, 由 (2.1) 式及 $a^{p^{n-1}} = b^{p^{m-1}}$ 推出

$$(a^{p^{n-m}} b^{-1})^{p^{m-1}} = (a^{p^{n-m}})^{p^{m-1}} (b^{-1})^{p^{m-1}} = a^{p^{n-1}} b^{-p^{m-1}} = 1.$$

令 $b' = a^{p^{n-m}} b^{-1}$. 则 $o(b') \leqslant p^{m-1} < o(b)$. 又 $o(\langle \bar{b'} \rangle) \leqslant o(b') \leqslant p^{m-1} \leqslant o(\bar{b})$. 另一方面, $\overline{G} = \langle \bar{a} \rangle \langle \bar{b'} \rangle$. 于是 $|\overline{G}| = |\langle \bar{a} \rangle \langle \bar{b} \rangle| = |\langle \bar{a} \rangle \langle \bar{b'} \rangle|$. 由此可得 $\frac{|\langle \bar{b} \rangle|}{|\langle \bar{a} \rangle \cap \langle \bar{b} \rangle|} = \frac{|\langle \bar{b'} \rangle|}{|\langle \bar{a} \rangle \cap \langle \bar{b'} \rangle|}$. 因为 $\langle \bar{a} \rangle \cap \langle \bar{b} \rangle = \bar{1}$ 及 $o(\langle \bar{b'} \rangle) \leqslant o(\bar{b})$, 推出 $\langle \bar{a} \rangle \cap \langle \bar{b'} \rangle = \bar{1}$. 故 b' 和 $a \pmod{G'}$ 仍然是 $\overline{G}$ 的基底, 但 $o(a)o(b') < o(a)o(b)$. 矛盾于 a, b 的选取.

若 $p = 2$, $m \geqslant 3$ 或 $n > m$, 则仍有 $(a^{p^{n-m}} b^{-1})^{p^{m-1}} = 1$. 同上可得矛盾. 于是 $n \leqslant m \leqslant 2$. 又由假设 $n \geqslant m$, 故有 $n = m = 2$. 因为 $a^{p^{n-1}} = b^{p^{m-1}} = d \in G'$, 故 $|\overline{G}| = |\langle \bar{a} \rangle \times \langle \bar{b} \rangle| \leqslant 2^{n-1} 2^{m-1}$. 从而 $|G| = |\overline{G}||G'| \leqslant 8$. 与我们假设 $|G| > p^3$ 矛盾. 事实上, $|G| = 8$ 且 $G \cong Q_8$.

这样我们证明了 $\langle a \rangle \cap \langle b \rangle = 1$. 并因此 $|G| \geqslant p^{n+m}$.

令 $[a, b] = c$. 则 $G' = \langle c \rangle$. 我们区分两种情况:

(i) G' 既不是 $\langle a \rangle$ 也不是 $\langle b \rangle$ 的子群:

此时因为 $|G'| = p$, 我们有 $\langle a \rangle \cap G' = 1$, $\langle b \rangle \cap G' = 1$. 于是 $\bar{a}^k = \bar{1} \Longleftrightarrow a^k \in \langle a \rangle \cap G' = 1$. 由此可得 $o(\bar{a}) = o(a)$. 同理, $o(\bar{b}) = o(b)$. 又 $G/G' = \overline{G} = \langle \bar{a} \rangle \times \langle \bar{b} \rangle$. 故 $|\overline{G}| = |\langle \bar{a} \rangle||\langle \bar{b} \rangle| = p^n p^m = p^{n+m}$. 则 $|G| = |\overline{G}||G'| = p^{n+m+1}$. 因为 $G' \leqslant Z(G)$, $n \geqslant m$, 此时我们有

$$a^{p^n} = b^{p^m} = c^p = 1, [a, b] = c, [c, a] = [c, b] = 1$$

且 $\exp G = p^n$, 其中 $n \geqslant m \geqslant 1$. 我们得到定理中的群 (iii). 由 $|G| = p^{n+m+1}$ 且 $\exp G = p^n$ 可知, n 和 m 都是 G 的不变量. 特别地, (iii) 型群中的不同参数的群互不同构.

(ii) G' 是 $\langle a\rangle$ 和 $\langle b\rangle$ 中恰好一个的子群:

如果我们去掉前面的假设 $n \geqslant m$, 则不妨设 $G' \leqslant \langle a\rangle$. 这时 $\langle a\rangle$ 是 G 的循环正规子群. 因为 $G/G' = \overline{G} = \langle\bar{a}\rangle \times \langle\bar{b}\rangle$, 故 $G = \langle a, b, G'\rangle = \langle a, b\rangle = \langle a\rangle\langle b\rangle$. 从而 G 是亚循环群. 因为 $G' \leqslant \langle a\rangle$, 故 $n \geq 2$. (否则, $G' = \langle a\rangle$). 设 $[a, b] = a^i$. 由定理 2.1.4 知 $Z(G) = \Phi(G) = \mho_1(G)G'$. 故 $b^p \in Z(G)$. 从而 $[a, b^p] = 1$. 因为 $G' \leqslant Z(G)$, 故 G 是类 2 的. 计算可得 $a^{ip} = [a, b]^p = [a, b^p] = 1$. 故可设 $i = sp^{n-1}$, $p \nmid s$. 设 t 满足 $st \equiv 1 (\mathrm{mod}\ p)$. 以 b^t 代替 b, 我们有 $o(b) = o(b^t)$, $G = \langle a, b\rangle = \langle a, b^t\rangle$. 因为 G 是类 2 的, 计算可得

$$[a, b^t] = [a, b]^t = (a^i)^t = (a^{sp^{n-1}})^t = a^{stp^{n-1}} = a^{(1+pt_1)p^{n-1}} = a^{p^{n-1}}.$$

不妨设 $b = b^t$. 则得到群的表现 (ii).

下面要证明 (ii) 型群中不同的参数值对应于不同构的群. 由 (2.1) 式和 $n \geq 2$ 可知, $\forall a, b \in G$, $(a^i b^j)^{p^{\max(m,n)}} = 1$. 故 $\exp G \leqslant p^{\max(m,n)}$. 又 $|G| = p^{n+m}$, 故 $\exp G = p^{\max(m,n)}$. 如果有与表现 (ii) 的群同构但参数不同的群, 它必有如下表现:

$$G = \langle a, b \mid a^{p^m} = b^{p^n} = 1, a^b = a^{1+p^{m-1}}\rangle, \qquad (ii')$$

并且 $n \neq m$. 在表现 (ii) 和 (ii') 的两个群中, 均有 $G' \leqslant \langle a\rangle$. 若 G 为表现 (ii) 的群, 下证 $G/G' \cong C_{p^{n-1}} \times C_{p^m}$. 首先, $G' = \langle [a, b]^g \mid g \in G\rangle = \langle a^{p^{n-1}}\rangle$. 故 $o(\bar{a}) = p^{n-1}$. 另一方面, $G = \langle a\rangle\langle b\rangle$. 从而 $G/G' = \overline{G} = \langle\bar{a}\rangle\langle\bar{b}\rangle$. 因为 $|G| = |\langle a\rangle\langle b\rangle| = \frac{|\langle a\rangle||\langle b\rangle|}{|\langle a\rangle \cap \langle b\rangle|} = |\langle a\rangle||\langle b\rangle|$. 故 $\langle a\rangle \cap \langle b\rangle = 1$. 由此得 $\langle\bar{a}\rangle \cap \langle\bar{b}\rangle = \bar{1}$. 从而 $G/G' = \overline{G} = \langle\bar{a}\rangle \times \langle\bar{b}\rangle$. 再一次由 $\langle a\rangle \cap \langle b\rangle = 1$ 得 $1 \neq b^{p^{m-1}} \notin G'$. 故 $o(\bar{b}) = o(b) = p^m$. 这就是说, $G/G' \cong C_{p^{n-1}} \times C_{p^m}$. 若 G 为表现 (ii') 的群, 同理可证, $G/G' \cong C_{p^{m-1}} \times C_{p^n}$. 此时, 一个 G/G' 有一个阶为 $\exp G$ 的循环正规子群, 而另一个没有. 显然这是一个矛盾.

最后我们证明 (ii) 型群和 (iii) 型群互不同构. 注意, 满足 $a, b \in G$ 使 $\bar{a} = aG', \bar{b} = bG'$ 是 $\overline{G} = G/G'$ 的基的所有 a, b 中 $o(a)o(b)$ 的最小

值显然也是 G 的一个不变量, 记其为 $m(G)$. 从证明中可以看出, (ii) 型群中 $|G|/m(G)=1$, (iii) 型群中 $|G|/m(G)=p$. □

§2.2 Dedikind p 群

称群 G 为**Dedekind 群**, 如果它的所有子群均在 G 中正规. 我们又称非交换的 Dedekind 群为**Hamilton 群**.

下面的定理给出了有限 Dedekind p 群的分类.

定理 2.2.1. 设 G 是有限 Dedekind p 群. 则

(1) G 交换; 或者

(2) $p=2$ 并且 $G\cong \mathrm{Q}_8\times \mathrm{C}_2^n$, 其中 n 是非负整数.

证明 设 $p>2$, G 是使定理不真的极小反例. 则 G 的每个真子群交换, 于是 G 是内交换群. 由定理 2.1.6, G 有非正规子群, 矛盾.

设 $p=2$, 且 G 非交换. 取 G 的一个内交换子群 H. 则 H 亦为 Dedekind 群, 由定理 2.1.6, $H\cong \mathrm{Q}_8$. 令 $H=\langle a,b\rangle$. 则 $o(a)=o(b)=4$, $a^2=b^2$, 且 $[a,b]=a^2$. 令 $C=C_G(H)$. 则 $C=C_G(\langle a\rangle)\cap C_G(\langle b\rangle)$. 由 N/C 定理, $|G:C_G(\langle a\rangle)|=2$, $|G:C_G(\langle b\rangle)|=2$. 于是 $|G:C|\leqslant 4$. 又, $C\cap H=Z(H)=\langle a^2\rangle$, 故 $HC=G$. 下面证 $\exp C=2$. 如若不然, 有 $c\in C$ 使得 $o(c)=4$. 因 G 中 2 阶子群皆正规, 故 2 阶元属于中心. 而因 $ac\notin Z(G)$, 推出 $o(ac)=4$. 又因 $[ac,b]=[a,b]=a^2$, $\langle ac\rangle\trianglelefteq G$, 有 $a^2\in\langle ac\rangle$. 于是得 $a^2=(ac)^2=a^2c^2$, $c^2=1$, 与 $o(c)=4$ 矛盾. 这样我们证明了 C 是初等交换 2 群. 取 $\langle a^2\rangle$ 在 C 中的补 D, 则 $G=H\times D$, 定理得证. □

第三章　亚循环 p 群

§3.1　亚循环 p 群的基本性质

称有限 p 群 G 是亚循环的, 若 G 有循环正规子群 N 使得 G/N 也是循环群. 亚循环群有以下重要的定理:

定理 3.1.1. 有限 p 群 G 亚循环当且仅当 $G/\Phi(G')G_3$ 亚循环.

证明　只需证充分性. 可设 $\Phi(G')G_3 \neq 1$. 取 $K \leqslant \Phi(G')G_3$ 满足 $|K| = p$, $K \trianglelefteq G$. 由归纳法可以假定 G/K 亚循环, 即存在 $L \trianglelefteq G$, $L \geqslant K$ 使得 G/L 和 L/K 是循环群. 如果 L 循环, 则 G 亚循环. 因此下面假设 L 不循环. 因为 $K \leqslant Z(G)$, L 交换. 设 $L = M \times K$, 其中 M 循环, 并且 $|M| = p^s$. 因为 $1 < \Phi(G')G_3 < G' < L$, $|L| \geqslant p^3$. 于是 $s \geqslant 2$. 又因 $\mho_1(M) = \mho_1(L)$ 以及 $L \trianglelefteq G$, $\mho_1(M) \trianglelefteq G$. 令 $N = \mho_1(M)K$. 则 $N \trianglelefteq G$ 且 $|L : N| = p$. 这推出 $L/N \leqslant Z(G/N)$. 因 G/L 循环, G/N 交换. 于是 $G' \leqslant N$. 因为

$$|G'/G' \cap \mho_1(M)| = |G'\mho_1(M)/\mho_1(M)| \leqslant |N/\mho_1(M)| = p,$$

有 $G' = G' \cap \mho_1(M)$ 或者 $|G' : G' \cap \mho_1(M)| = p$. 假定前者发生, $K \leqslant G' \leqslant \mho_1(M) < M$, 矛盾. 于是有 $|G' : G' \cap \mho_1(M)| = p$. 又因 $G' \cap \mho_1(M) \trianglelefteq G$, 设 $\overline{G} = G/G' \cap \mho_1(M)$, 有 $|\overline{G}'| = p$. 于是 $\Phi(\overline{G}') = \bar{1}$, $\overline{G}_3 = \bar{1}$. 这得到 $\Phi(G')G_3 \leqslant G' \cap \mho_1(M)$. 但因 $K \leqslant \Phi(G')G_3$, 得 $K \leqslant G' \cap \mho_1(M) < M$, 矛盾. □

定理 3.1.2. 对于 $p > 2$, 有限 p 群 G 亚循环当且仅当 $\omega(G) \leqslant 2$.

证明　$\Longrightarrow$: 因 G 亚循环, $G' \leqslant \mho_1(G)$, 即 $\mho_1(G) = \Phi(G)$. 于是

$$p^{\omega(G)} = |G/\mho_1(G)| = |G/\Phi(G)| \leqslant p^2,$$

即 $\omega(G)\leqslant 2$.

$\Longleftarrow$: 对任意的 $N\trianglelefteq G$, $(G/N)/\mho_{(}G/N)=(G/N)/(\mho_{(}G)N/N)\cong G/\mho_{(}G)N$, 因此 $\omega(G/N)\leqslant\omega(G)$. 由定理 3.1.1, 可设 $\Phi(G')G_3=1$. 因此 G 内交换. 又因 $\omega(G)\leqslant 2$,

$$|G/\Phi(G)|\leqslant|G/\mho_1(G)|\leqslant p^2.$$

除掉 G 循环的情形, 有 $d(G)=2$ 和 $\Phi(G)=\mho_1(G)$. 因此 $G'\leqslant\mho_1(G)$. 这时 G 是定理 2.1.6 中的 (2) 型群. 因此 G 亚循环. □

推论 3.1.3. (Huppert) 对于 $p>2$, 若有限 p 群 G 可表为二循环子群的乘积: $G=\langle a\rangle\langle b\rangle$, 则 G 亚循环.

证明 由推论条件, $\mho_1(G)\geqslant\langle a^p\rangle\langle b^p\rangle$, 故 $|G/\mho_1(G)|\leqslant p^2$, 即 $\omega(G)\leqslant 2$. 由定理 3.1.2 即得结论. □

§3.2 亚循环 p 群和内亚循环群 p 群的分类

有关亚循环 p 群的研究成果是相当丰富的. 从上世纪 60 年代末开始, 已有许多人给出了亚循环 p 群的分类. 然而有限亚循环 p 群分类的是 1973 年 B. W. King 第一个在文 [43] 中给出的. 因为其发表得最早, 这个结果得到了广泛的应用. 但是遗憾的是, B. W. King 的分类中有两个小错误. 这两个小错误最早是 1987 年, 被徐明曜在文 [61] 中指出. 随后 G. L. Peterson 和 G. Silberberg 分别在文 [53, 59] 对错误进行了纠正. 另外, 在 [49, 50, 51] 中, M. F. Newman 和徐明曜利用 p 群生成算法重新分类了亚循环 p 群, 其中 $p>2$ 的情形已经发表, 见 [50]; 但 $p=2$ 的情形尚未发表. 对于 $p=2$ 的情形, 在 [62] 中, 徐明曜、张勤海完整地分类了亚循环 2 群, 其方法完全独立于 p 群生成算法. 下面我们的定理阐述了文 [50, 51, 4, 62] 给出的亚循环 p 群的分类.

定理 3.2.1. (1) 设 G 是亚循环 p 群, p 为奇素数, 则

$$G=\langle a,b \mid a^{p^{r+s+u}}=1, b^{p^{r+s+t}}=a^{p^{r+s}}, a^b=a^{1+p^r}\rangle$$

其中 r,s,t,u 是非负整数且满足 $r\geqslant 1, u\leqslant r$, 对于参数 r,s,t,u 的不同取值, 对应的亚循环群互不同构, 我们用 $<r,s,t,u>_p$ 来记这个群.

(2) 设 G 是亚循环 2 群, 则 G 是以下群之一:

(I) G 有一个循环极大子群. 则 G 是二面体群, 半二面体群, 广义四元数群, 或一般亚循环群 $G=\langle a^{2^n}=1, b^2=1, a^b=a^{1+2^{n-1}}\rangle, n\geqslant 3$.

接下来我们假设 G 没有循环极大子群. 则 G 是以下互不同构的两种群之一:

(II) 通常的亚循环 2 群: $G=\langle a,b \mid a^{2^{r+s+u}}=1, b^{2^{r+s+t}}=a^{2^{r+s}}, a^b=a^{1+2^r}\rangle$, 其中 r,s,t,u 是非负整数且满足 $r\geqslant 2, u\leqslant r$, 对于参数 r,s,t,u 的不同取值, 对应的亚循环群互不同构, 我们用 $<r,s,t,u>_2$ 来记这个群.

(III) 特殊的亚循环 2 群: $G=\langle a,b \mid a^{2^{r+s+v+t'+u}}=1, b^{2^{r+s+t}}=a^{2^{r+s+v+t'}}, a^b=a^{-1+2^{r+v}}\rangle$, 其中 r,s,v,t,t',u 是非负整数且满足 $r\geqslant 2, t'\leqslant r, u\leqslant 1, tt'=sv=tv=0$, 而且若 $t'\geqslant r-1$, 则 $u=0$. 我们用 $<r,s,v,t,t',u>_2$ 来表示这个群. 不同类型的群互不同构, 同一种类型但参数具有不同值的群互不同构.

下面是内亚循环群的分类.

定理 3.2.2. (Blackburn [18]) 设 G 是内亚循环 p 群. 则 G 是下列群之一:

(1) p^3 阶初等交换群;

(2) 方次数为 p 的 p^3 阶非交换群, 其中 p 是奇数;

(3) 幂零类为 3 的 3^4 阶群: $\langle a,b,c \mid b^9=c^3=1, [c,b]=1, a^3=b^{-3}, [b,a]=c, [c,a]=b^{-3}\rangle$.

(4) $Q_8 \times C_2$ 或者 $D_8 * C_4$(阶为 16). $D_8 * C_4 = \langle a, b, d \mid a^2 = b^2 = d^4 = 1, [a, b] = d^2, [d, a] = [d, b] = 1 \rangle$;

(5) $\langle a, b, c \mid a^4 = b^4 = 1, c^2 = a^2b^2, [a, b] = b^2, [c, a] = a^2, [c, b] = 1 \rangle$ 且阶为 32.

第四章　指数为 p^2 的子群都交换的有限 p 群

显然, 指数为 p^2 的子群都交换的有限非交换 p 群一定是有限亚 Hamilton p 群. 这样的 p 群包括内交换 p 群和 $\mathcal{A}_2$ 群.

我们以 $\mathcal{P}$ 表示任一群性质, 比如可解, 交换, 循环, 亚循环等等. 称群 G 为 $\mathcal{P}$ 群, 如果 G 具有性质 $\mathcal{P}$. 若群 G 不是 $\mathcal{P}$ 群, 但 G 的每个真子群皆为 $\mathcal{P}$ 群, 则称 G 是一个内 $\mathcal{P}$ 群.

设 G 是有限 p 群. 我们称 G 是 $\mathcal{P}_n$ 群, 若 G 的所有指数为 p^n 的子群都是 $\mathcal{P}$ 群, 并且至少有一个指数为 p^{n-1} 的子群不是 $\mathcal{P}$ 群.

特别地, 我们用 $\mathcal{A}$ 来表示 "交换" 这一群性质. 则 $\mathcal{A}_1$ 群是指所有极大子群都交换但本身非交换的有限 p 群, 即内交换 p 群. $\mathcal{A}_2$ 群是指所有 2 极大子群都交换但至少有一个极大子群非交换的有限 p 群.

§4.1　亚循环 $\mathcal{A}_2$ 群的分类

首先假设 G 亚循环. 为了分类 $\mathcal{A}_2$ 群, 我们给出定理 4.1.1.

定理 4.1.1. 设 G 是亚循环 p- 群. 则 $G \in \mathcal{A}_2$ 当且仅当 $|G'| = p^2$.

证明　设 G 是 $\mathcal{A}_2$ 群. G 的极大子群交换或极小非交换. 设 M 是非交换的极大子群. 则 M 极小非交换. 由定理 2.1.4, $|M'| = p$. 因为 G' 是循环群以及 $M' \leqslant G'$, 得到 $M' = \Omega_1(G')$. 设 $\overline{G} = G/M' = G/\Omega_1(G')$. 断言 $\overline{G}' \neq 1$. 若否, $G' = \Omega_1(G')$ 且阶为 p. 由 G 是亚循环群, 有 $d(G) = 2$. 根据定理 2.1.4, G 是 $\mathcal{A}_1$ 群, 矛盾. 由 $K/\Omega_1(G')$ 是极大子群可知, K 是极大子群. 由 $K' \leqslant \Omega_1(G')$, $K/\Omega_1(G')$ 是交换群. 由定理 2.1.4, $\overline{G}$ 是 $\mathcal{A}_1$ 群. 我们推的 $|G'/\Omega_1(G')| = |\overline{G}'| = p$. 故 $|G'| = p^2$.

反过来, 假设 $|G'| = p^2$. 设 $N = \Omega_1(G')$, H 是 G 的一个极大子群. 则 $G' \leqslant \Phi(G) \leqslant H$. 若 $G' = H$, 则存在元素 $a \in G \backslash H$ 满足 $G = \langle H, a \rangle$. 这样 $G = \langle G', a \rangle = \langle a \rangle$ 是交换群, 矛盾. 因此 $N < G' < H$. 因为 $|G'/N| = p$ 和 $d(G/N) = d(G) = 2$, 所以, 由定理 2.1.4, G/N 是内交换

群. 这样, H/N 交换, 因而 $H' \leqslant N$. 故 $H' = 1$ 或 $H' = N$. 若 $H' = N$, 则 $|H'| = p$. 又 G 是亚循环, 那么 $d(H) = 2$. 由定理 2.1.4, H 是内交换群. 因此, G 是 $\mathcal{A}_2$ 群. □

根据定理 4.1.1, 我们将找出定理 3.2.1 中满足 $\mathcal{A}_2$ 群条件的群. 有以下定理

定理 4.1.2. *设 G 是亚循环 p- 群. 则 G 是 $\mathcal{A}_2$ 群当且仅当 G 是以下互不同构的群之一:*

(1) $< r, s, t, u >_p$ 满足 $s + u = 2$, 并且若 $p = 2$, 则 $r \geqslant 2$.

(2) 16 阶二面体群, 半二面体群和广义四元数群.

(3) $< r, s, v, t, t', u >_2$ 其中 $r = 3$, $s = v = t' = u = 0$, $t \geqslant 0$.

(4) $< r, s, v, t, t', u >_2$ 其中 $r = 2$, $s + v + t' + u = 1$, $t \geqslant 0$.

证明 (1) 假设 $p > 2$. 由定理 3.2.1, $G' = \langle a^{p^r} \rangle$. 由于 G 是 $\mathcal{A}_2$ 群, G' 的阶为 p^2, 即 $|G'| = p^{s+u} = p^2$ 且 $s + u = 2$. 同样, 当 G 是通常的亚循环 2 群时, 我们得到相同的结果.

(2) 假设 G 有循环极大子群且 $|G| = 2^{n+1}$. 这些群如下所示

二面体群 $G = \langle a, b \mid a^{2^n} = b^2 = 1, b^{-1}ab = a^{-1} \rangle$ 其中 $n \geqslant 2$.

半二面体群 $G = \langle a, b \mid a^{2^n} = b^2 = 1, b^{-1}ab = a^{-1+2^{n-1}} \rangle$ 其中 $n \geqslant 3$,

广义四元数群 $G = \langle a, b \mid a^{2^n} = 1, b^2 = a^{2^{n-1}}, b^{-1}ab = a^{-1} \rangle$ 其中 $n \geqslant 2$,

这三种群都是极大类 2- 群. 注意到 $G' = \langle a^2 \rangle$ 且阶为 2^{n-1}. 由 G 是 $\mathcal{A}_2$ 群, $|G'| = p^2$. 故 $n = 3$, $|G| = 16$.

对于一般的亚循环 2- 群, $G = \langle a, b \mid a^{2^n} = 1, b^2 = 1, a^b = a^{1+2^{n-1}} \rangle$. 其中 $n \geqslant 3$. $G' = \langle a^{2^{n-1}} \rangle$ 且阶为 2. 又因为 $d(G) = 2$. 根据引理 2.1.4, G 是内交换群.

(3) 设 G 是特殊亚循环 2 群.

$G' = \langle a^2 \rangle$ 且阶为 $2^{r+s+v+t'+u-1}$. 因为 G 是 $\mathcal{A}_2$ 群, 所以 $r+s+v+t'+u-1=2$. 若 $r=3$, 则 $s=v=t'=u=0$, $t \geqslant 0$; 若 $r=2$, 则 $s+v+t'+u=1$, $t \geqslant 0$. □

§4.2 p^4 阶 $\mathcal{A}_2$ 群的分类

假设 G 非亚循环. 既然 p^4 阶群的分类已被人们所知, 那么只需要找出此分类中的非亚循环 $\mathcal{A}_2$ 群.

定理 4.2.1. *设 G 是 p^4 阶群. 则 G 同构于以下群之一:*

一、G 为交换群:

(1) $G \cong C_{p^4}$;

(2) $G = \langle a, b \mid a^{p^3} = b^p = 1, [a, b] = 1 \rangle$;

(3) $G = \langle a, b \mid a^{p^2} = b^{p^2} = 1, [a, b] = 1 \rangle$;

(4) $G = \langle a, b, c \mid a^{p^2} = b^p = c^p = 1, [a, b] = [a, c] = [b, c] = 1 \rangle$;

(5) $G \cong C_p^4$.

二、G 为非交换群 ($p = 2$):

(6) 广义四元数群 $G = \langle a, b \mid a^{2^3} = 1, b^2 = a^4, b^{-1}ab = a^{-1} \rangle$;

(7) 二面体群 $G = \langle a, b \mid a^{2^3} = b^2 = 1, b^{-1}ab = a^{-1} \rangle$;

(8) $G = \langle a, b \mid a^{2^3} = b^2 = 1, b^{-1}ab = a^5 \rangle$;

(9) 半二面体群 $G = \langle a, b \mid a^{2^3} = b^2 = 1, b^{-1}ab = a^3 \rangle$;

(10) $G \cong D_8 \times C_2$;

(11) $G = \langle a, b \mid a^4 = b^4 = 1, b^{-1}ab = a^{-1} \rangle$;

(12) $G \cong D_8 * C_4$;

(13) $G \cong Q_8 \times C_2$;

(14) $G = \langle a, b, c \mid a^4 = b^2 = c^2 = 1, [a, b] = c, [a, c] = [b, c] = 1 \rangle$;

三、G 为非交换群 ($p > 2$):

(6) $G=\langle a,b \mid a^{p^3}=b^p=1, b^{-1}ab=a^{1+p^2}\rangle$;

(7) $G\cong M\times C_p$, 其中 M 是 p^3 阶非交换群且 $\exp M=p^2$;

(8) $G=\langle a,b \mid a^{p^2}=b^{p^2}=1, b^{-1}ab=a^{1+p}\rangle$;

(9) $G=\langle a,b,c \mid a^{p^2}=b^p=c^p=1, [b,c]=a^p, [a,b]=[a,c]=1\rangle$;

(10) $G=\langle a,b,c \mid a^{p^2}=b^p=c^p=1, [a,b]=c, [a,c]=[b,c]=1\rangle$;

(11-13) $G=\langle a,b,c \mid a^{p^2}=b^p=1, c^p=a^{\alpha p}, [a,b]=a^p, [a,c]=b, [b,c]=1\rangle$, 其中 $\alpha=0,1$ 或 α 是一个固定的模 p 的平方非剩余; 当 α 取不同的值时, 决定 3 种互不同构的群.

(14) $G\cong M\times C_p$, 其中 M 是 p^3 阶非交换群且 $\exp M=p$;

(15) $G=\langle a,b,c,d \mid a^p=b^p=c^p=d^p=1, [c,d]=b, [b,d]=a, [a,b]=[a,c]=[a,d]=[b,c]=1\rangle$, 其中 $p>3$;

(16) $G=\langle a,b,c \mid a^9=b^3=c^3=1, [a,b]=1, [a,c]=b, [c,b^{-1}]=a^{-3}\rangle$.

定理 4.2.2. 设 G 是 $\mathcal{A}_2$ 群且 $|G|=p^4$. 假设 G 非亚循环. 则

(1) 若 $p=2$, G 是 $D_8\times C_2$, 或 $Q_8\times C_2$, 或中心积 D_8*C_4.

(2) 若 $p>2$, G 是 $M\times C_p$, 其中 M 为 p^3 阶非交换群 (M 有两种互不同构的形式), 或以下互不同构的群之一:

(i) $\langle a,b,c \mid a^{p^2}=b^p=c^p=1, [b,c]=a^p, [a,b]=[a,c]=1\rangle$;

(ii) $\langle a,b,c,d \mid a^p=b^p=c^p=d^p=1, [c,d]=b, [b,d]=a, [a,b]=[a,c]=[a,d]=[b,c]=1\rangle$;

(iii) $\langle a,b,c \mid a^{p^2}=b^p=1, c^p=a^{\alpha p}, [a,b]=a^p, [a,c]=b, [b,c]=1\rangle$, 其中 $\alpha=0,1$ 或是一个模 p 的平方非剩余 (三种互不同构的群);

(iv) $p=3$, $\langle a,b,c \mid a^9=b^3=c^3=1, [a,b]=1, [a,c]=b, [c,b^{-1}]=a^{-3}\rangle$.

证明 我们只需考虑定理 4.2.1 中的非交换群. 因为 $|G|=p^4$, 所以 G 的指数为 p^2 的子群都交换. 由 $\mathcal{A}_2$ 群的定义, G 是 $\mathcal{A}_2$ 群等价于

G 有一个非交换的极大子群, 也等价于 G 不是内交换群.

设 $p=2$. 群 (8), (11) 和 (14) 都是内交换群. 对于群 (6), (7) 和 (9), 由于 $G'=\langle a^2\rangle$ 且阶为 4, 故它们都是亚循环的 $\mathcal{A}_2$ 群. 对于群 (10), (12) 和 (13), 它们都是三元生成的, 根据定理 2.1.4 可知, 它们都不是内交换群, 因此这三种类型的群都是 $\mathcal{A}_2$ 群.

接下来考虑 $p>2$ 的情况. 群 (6), (8) 和 (10) 都是内交换群. 群 (7), (9), (14) 都是二元生成的; 对于群 (11–13), $G=\langle a,c\rangle$, $G'=\langle a^p,b\rangle$ 且阶是 p^2; 对于群 (15), $G=\langle c,d\rangle$, $G'=\langle a,b\rangle$ 且阶为 p^2; 对于群 (16), $G=\langle a,c\rangle$, $G'=\langle b,a^3\rangle$ 且阶为 9. 根据定理 2.1.4 可知, 群 (7), (9), (11–13), (14), (15), (16) 都不是内交换群, 故都是 $\mathcal{A}_2$ 群.

通过以上的计算, 我们知道: 当 $p=2$ 时, 群 (10), (12) 和 (13) 是非亚循环 $\mathcal{A}_2$ 群; 当 $p>2$ 时, 群 (7), (9), (11-16) 是非亚循环 $\mathcal{A}_2$ 群. 进一步地, 当 $p=2$ 时, 群 (10), (12) 和 (13) 是定理 4.2.2(1) 中的群. 群 (7) 或 (14) 是定理 4.2.2(1) 中的群 $M\times C_p$, $p>2$; 群 (9) 是 (i) 型群; 群 (15) 是 (ii) 型群; 群 (11-13) 是 (iii) 型群, 以及群 (16) 是 (iv) 型群.□

§4.3 二元生成有交换极大子群的 $\mathcal{A}_2$ 群的分类

以下假设 $|G|\geqslant p^5$ 且 G 有非交换的极大子群. 先给出两个有用的引理.

引理 4.3.1. 设 G 是一个非交换 p- 群且有一个交换的极大子群和一个非交换的极大子群.

(1) 设 K 是 G 的非交换的极大子群. 则 $|G':K'|=p|Z(K)|/|Z(G)|$;

(2) 若 $d(G)=2$, $c(G)\geqslant 3$.

证明 (1) 由定理 2.1.3, $|G|=p|G'||Z(G)|$. 设 A 是 G 的交换的极大子群. 则 $G=KA$. 因为 $|G/A|=|KA/A|=|K/K\cap A|=p$, 所以 $K\cap A$ 是 K 的交换极大子群. 由定理 2.1.3, $|K|=p|K'||Z(K)|$. 故 $|G':K'|=p|Z(K)|/|Z(G)|$. 结论成立.

(2) 若否, 设 A 是 G 的交换极大子群. 设 $G=\langle a,b\rangle$, 其中 $a\in A$. 由 $c(G)=2$ 和 $b^p\in A$ 可得, $[a,b]^p=[a,b^p]=1$. 则 $|\langle[a,b]\rangle|=|G'|=p$. 根据定理 2.1.4, G 是 $\mathcal{A}_1$ 群, 矛盾. □

引理 4.3.2. 设 G 是 $\mathcal{A}_2$ 群, $\mathrm{d}(G)=2$, 且 $|G|=p^n$, G 有一个交换的极大子群 A, 非交换的极大子群 K. 则

(1) $\mathrm{Z}(K)=\Phi(K)=\mathrm{Z}(G)$, $|G'|=p^2$, $c(G)=3$, 以及 $G'\cap\mathrm{Z}(G)=G_3$;

(2) 对于 $b\in G\backslash A$, $G=\langle b,A\rangle$, $\mathrm{Z}(G)=\langle b^p,G_3\rangle$ 以及 $o(bG')=o(bG_3)=p^{n-3}$, 存在元素 a_1 满足 $a_1\in A\backslash\Phi(G)$ 且 $o(a_1G')=p$.

证明 (1) 因为 G 非交换和 $\mathrm{d}(G)=2$, 所以 $\mathrm{Z}(G)\leqslant\Phi(G)<K$, 进而 $\mathrm{Z}(G)\leqslant\mathrm{Z}(K)$. 又由 $G=\langle A,K\rangle$ 和 $\Phi(K)=Z(K)\leqslant A$ 可得, $Z(K)\leqslant Z(G)$. 因此 $Z(K)=Z(G)$. 根据引理 4.3.1, $|G'|=p^2$, $c(G)=3$. 因为 $G_3\leqslant Z(G)$, 所以 $G_3\leqslant Z(G)\cap G'$. 又因为 $c(G)=3$, 故 $G_3=Z(G)\cap G'$.

(2) 因为 A 是 G 的交换极大子群以及 $b\in G\backslash A$, 所以 $G=\langle b,A\rangle$, 也有 $\mathrm{Z}(G)=C_A(b)$. 若否, $\mathrm{Z}(G)<C_A(b)$. 存在 $x\in C_A(b)\backslash Z(G)$. 故 $x\in Z(G)$, 矛盾. 设 $M=\langle b,G'\rangle$. 由 $c(G)=3$ 可得, M 非交换. 这样, M 是极大子群并且是极小非交换. 设 $\overline{G}=G/G_3$. 因为 $d(\overline{G})=d(G)=2$ 和 $|\overline{G}'|=p$, 所以 $\overline{G}$ 是内交换群. 再由 M/G_3 交换, $M'=G_3$. 则 $\langle b^p,G_3\rangle\leqslant\Phi(M)$.

因为 $|M/\langle b^p,G_3\rangle|=|\langle b,G'\rangle/\langle b^p,G_3\rangle|=p^2$, 所以 $\langle b^p,G_3\rangle=\Phi(M)$. 由定理 2.1.4, $\mathrm{Z}(M)=\Phi(M)=\langle b^p,G_3\rangle$ 且由 (1) 有 $\mathrm{Z}(G)=\langle b^p,G_3\rangle$.

设 $\langle b^p\rangle\cap G_3=\langle b^{p^t}\rangle$. 由 $|Z(G)|=\frac{|\langle b^p\rangle||G_3|}{|\langle b^p\rangle\cap G_3|}=\frac{|\langle b^p\rangle||G_3|}{|\langle b^{p^t}\rangle|}=p^t=p^{n-3}$ 可得 $t=n-3$ 且 $\langle b^p\rangle\cap G_3=\langle b^{p^{n-3}}\rangle$. 因此 $o(bG_3)=p^{n-3}$. 因为 $b^p\in C_A(b)=\mathrm{Z}(G)$ 和 $Z(G)\cap G'=G_3$, 所以 $\langle b^p\rangle\cap G'\leqslant\langle b^p\rangle\cap G_3$. 又 $\langle b^p\rangle\cap G'\geqslant\langle b^p\rangle\cap G_3$, 所以 $\langle b^p\rangle\cap G'=\langle b^p\rangle\cap G_3$. 故 $o(bG')=o(bG_3)$, 也有 G/G' 的型不变量为 (p^{n-3},p). 存在元 a_1 满足 $o(a_1G')=p$ 且

$G/G' = \langle bG', a_1G'\rangle$. 我们断言 $a_1 \in A$. 若 $a_1 \notin A$, $o(a_1G') = p^{n-3} > p$. 矛盾. 由 $G = \langle b, a_1, G'\rangle = \langle b, a_1\rangle$, $a_1 \notin \Phi(G)$. □

以下定理 4.3.3, 我们列出了所有的有交换极大子群的二元生成的 $\mathcal{A}_2$ 群.

定理 4.3.3. 设 G 是二元生成的 $\mathcal{A}_2$ 群且有一个交换的极大子群 A. 假设 G 非亚循环且 $|G| = p^n$ $(n \geqslant 5)$, 则 $p > 2$, 且 G 是以下群之一:

(1) $\langle b, a_1, a_2, a_3 \mid b^{p^{n-3}} = a_1^p = a_2^p = a_3^p = 1, [a_1, b] = a_2, [a_2, b] = a_3, [a_i, a_j] = 1, [a_3, b] = 1\rangle$, 其中 $1 \leqslant i, j \leqslant 3$;

(2) $\langle b, a_1, a_2 \mid b^{p^{n-2}} = a_1^p = a_2^p = 1, [a_1, b] = a_2, [a_2, b] = b^{p^{n-3}}, [a_1, a_2] = 1, [b^{p^{n-3}}, a_1] = [b^{p^{n-3}}, a_2] = 1\rangle$;

(3) $\langle b, a_1, a_2 \mid b^{p^{n-3}} = a_1^{p^2} = a_2^p = 1, [a_1, b] = a_2, [a_2, b] = a_1^{\nu p}, [a_1, a_2] = 1, [a_1^p, b] = [a_1^p, a_2] = 1\rangle$, 其中 $\nu = 1$ 或者 ν 是一个固定的模 p 的平方非剩余.

证明 设 $G = \langle a_1, b\rangle$ 其中 $b \in G\backslash A, a_1 \in A\backslash\Phi(G)$. 由定理 4.3.2, 我们假设 $a_1^p \in G'$. 设 $a_2 = [a_1, b]$ 和 $a_3 = [a_2, b]$. 则 $G' = \langle a_2, a_3\rangle$ 且 $[a_i, a_j] = 1$ 其中 $i, j = 1, 2, 3$. 由 $b^p \in A$, 我们有 $[a_1, b^p] = 1$ 和 $[a_2, b^p] = 1$. 计算可得 $a_2^{\binom{p}{1}}a_3^{\binom{p}{2}} = 1$ 且 $a_3^p = 1$.

我们断言 $p > 2$. 若否, $a_3^2 = 1$ 和 $a_3 = a_2^{-2}$. 计算可得 $[a_1^2a_2, b] = a_2^2a_3 = 1$, 我们有 $a_1^2a_2 \in \mathrm{Z}(G)$. 根据引理 4.3.2(2), $a_1^2 \in G'$. 因此 $a_1^2a_2 \in G' \cap \mathrm{Z}(G) = G_3$. 则 $a_1^2a_2 = 1$ 或 $a_1^2a_2 = a_2^{-2}$. 容易得到 $a_2 = a_1^{-2}$ 或 $a_2 = a_1^2$. 因为 $a_1^b = a_1[a_1, b] \in \langle a_1\rangle$, 所以 $\langle a_1\rangle$ 是 G 的正规子群. 故 $G = \langle a_1\rangle\langle b\rangle$ 亚循环, 矛盾与假设.

因为 $p > 2$, 所以 $a_2^p = 1, a_3^p = 1$, 因此 $\exp(G') = p$. 由 $[a_1^p, b] = [a_1, b]^p[2a_1, b]^{\binom{p}{2}} = a_2^p = 1$, 有 $a_1^p \in \mathrm{Z}(G)$. 又 $a_1^p \in G'$, 所以 $a_1^p \in G' \cap \mathrm{Z}(G) = G_3 = \langle a_3\rangle$. 设 $a_1^p = a_3^x$. 由 $o(bG_3) = p^{n-3}$, 设 $b^{p^{n-3}} = a_3^y$, 其中 $0 \leqslant x, y \leqslant p-1$.

若 $x = y = 0$, 则 G 是类型 (1).

若 $(y, p) = 1$. 设 $a_1' = a_1 b^{-xy'p^{n-4}}$. 其中 $yy' \equiv 1 (\bmod p)$. 那么 $a_1' \in A \backslash \Phi(G), a_2' = a_2, a_3' = a_3$. 故 $a_1'^p = a_1^p b^{-xy'p^{n-3}} = 1$. 在此情况下. 我们假设 $x = 0$. 设 $a_1' = a_1^y$. 则 $a_3' = [a_1', b, b] = [a_1^y, b, b] = [a_1, b, b]^y = a_3^y = b^{p^{n-3}}$. 用 a_1' 代替 a_1, G 同构于类型 (2).

若 $y = 0$ 且 $(x, p) = 1$, 设 $b' = b^k$, 其中 $(k, p) = 1$. 那么 $a_3' = [a_1, b', b'] = [a_1, b^k, b^k] = [a_1, b, b]^{k^2} = a_3^{k^2} = a_1^{k^2 x' p}$ 其中 $xx' \equiv 1 (\bmod p)$. 若 x' 是模 p 的平方剩余, 设 $k^2 = x$ 且满足 $k^2 x' \equiv 1 (\bmod p)$; 若 x' 是模 p 的平方非剩余, 设 $x' = (t)^{2n+1}, k = (t)^{-n}$, 其中 t 是模 p 的原根. 故 $a_1^{k^2 x' p} = a_1^{tp}$. 进一步地, 假设 t 是一个固定的模 p 的平方非剩余. 用 b' 代替 b, 则 G 同构于以下两种群之一:

(3a) $G = \langle a_1, b \mid b^{p^{n-3}} = a_1^{p^2} = a_2^p = 1, [a_1, b] = a_2, [a_2, b] = a_1^p,$
$[a_1, a_2] = 1, [a_1^p, b] = [a_1^p, a_2] = 1 \rangle$,

(3b) $G = \langle a_1, b \mid b^{p^{n-3}} = a_1^{p^2} = a_2^p = 1, [a_1, b] = a_2, [a_2, b] = a_1^{tp},$
$[a_1, a_2] = 1, [a_1^p, b] = [a_1^p, a_2] = 1 \rangle$,

接下来, 我们验证类型 (1), (2), (3a), (3b) 的群都是 $\mathcal{A}_2$ 群. 其实就是验证极大子群中既有交换群, 也有非交换群, 并且非交换的都是 $\mathcal{A}_1$ 群. 对于每一种类型的群都有 $c(G) = 3$, $\exp(G') = p$ 和 $|G'| = p^2$. 由 $d(G) = 2$, G 有 $p+1$ 个极大子群. 极大子群分别是 $\langle a_1, \Phi(G) \rangle$ 和 $K_s = \langle ba_1^s, \Phi(G) \rangle$, (其中 $s = 0, 1, \ldots, p-1$).

对于类型 (1) $Z(G) = \langle b^p, a_3 \rangle$, $\Phi(G) = \langle b^p, a_2, a_3 \rangle = \langle a_2, Z(G) \rangle$. 极大子群如下:

$H = \langle a_1, \Phi(G) \rangle = \langle a_1, a_2, Z(G) \rangle$ 是交换群.

$K_s = \langle ba_1^s, \Phi(G) \rangle = \langle ba_1^s, b^p, a_2, a_3 \rangle$, $(s = 0, 1, \ldots, p-1)$.

因为 $(ba_1^s)^p = b^p a_1^{sp} [b, a_1^{-s}]^{\binom{p}{2}} [b, 2a_1^{-s}]^{\binom{p}{3}} \ [2b, a_1^{-s}]^{\binom{p}{3}} = b^p a_3^{s\binom{p}{3}}$ 和 $[a_2, ba_1^s] = a_3$, 所以 $|K_s'| = |\langle a_3 \rangle| = p$, $\langle (ba_1^s)^p, a_3 \rangle = \langle b^p, a_3 \rangle = \Phi(K_s)$, 而且 $d(K_s) = 2$. 由引理 2.1.4, $K_s = \langle ba_1^s, a_2 \rangle$ 是内交换群.

对于类型 (2) $Z(G)=\langle b^p\rangle$, $\Phi(G)=\langle b^p, a_2\rangle=\langle a_2, Z(G)\rangle$. 极大子群如下:

$H=\langle a_1,\Phi(G)\rangle=\langle a_1,a_2,Z(G)\rangle$ 是交换群.

$K_s=\langle ba_1^s,\Phi(G)\rangle=\langle ba_1^s,b^p,a_2\rangle$ $(s=0,1,\ldots,p-1)$. 因为 $(ba_1^s)^p=b^pa_3^{s\binom{p}{3}}=b^pb^{sp^{n-3}\binom{p}{3}}$ 和 $[a_2,ba_1^s]=a_3=b^{p^{n-3}}\leqslant\langle(ba_1^s)^p\rangle$, 所以 $|K_s'|=|\langle b^{p^{n-3}}\rangle|=p$, $\langle(ba_1^s)^p,b^{p^{n-3}}\rangle=\langle b^p\rangle=\Phi(K_s)$, 而且有 $d(K_s)=2$. 因此 $K_s=\langle ba_1^s,a_2\rangle$ 是内交换群.

对于类型 (3) $Z(G)=\langle b^p,a_1^p\rangle$, $\Phi(G)=\langle b^p,a_1^p,a_2\rangle=\langle a_2,Z(G)\rangle$. 极大子群如下:

$H=\langle a_1,\Phi(G)\rangle=\langle a_1,a_2,Z(G)\rangle$ 是交换群.

$K_s=\langle ba_1^s,\Phi(G)\rangle=\langle ba_1^s,b^p,a_1^p,a_2\rangle$, $(s=0,1,\ldots,p-1)$. 因为 $(ba_1^s)^p=b^pa_3^{s\binom{p}{3}}=b^pa_1^{\nu sp\binom{p}{3}}$ 和 $[a_2,ba_1^s]=a_1^{\nu p}$, 所以 $|K_s'|=|\langle a_1^p\rangle|=p$, $\langle(ba_1^s)^p,a_1^p\rangle=\langle b^p,a_1^p\rangle=\Phi(K_s)$, 而且有 $d(K_s)=2$. 因此 $K_s=\langle ba_1^s,a_2\rangle$ 是内交换群.

这样就证明了以上四种群都是 $\mathcal{A}_2$ 群.

最后, 我们证明类型 (1), (2), (3a) 和 (3b) 的群互不同构. 设 $g=b^xa_1^ya_2^za_3^w$. $g^p=(b^xa_1^ya_2^za_3^w)^p\equiv b^{xp}a_1^{yp}(\mathrm{mod}\ G_3)$. 存在元素 g_0 ($(x,p)=1$) 满足 $g_0^p\neq 1$ 且 $g_0^{p^2}=b^{xp^2}$. 则 $o(g_0)=o(b)$ 是群 G 中的最高阶元. 因此 $\exp(G)=o(b)$. 对于群 (2), $\exp(G)=p^{n-2}$, 但对于其它类型的群而言, $\exp(G)=p^{n-3}$. 接下来, 考虑唯一的交换极大子群 A. 对于群 (1), $A=\langle b^p,a_1,a_2,a_3\rangle$. 通过计算, $\frac{A}{\Phi(A)}=\frac{A}{\langle b^{p^2}\rangle}$, 且 $\frac{|A|}{|\Phi(A)|}=\frac{p^{n-1}}{p^{n-5}}=p^4$. 故 $\mathrm{d}(A)=4$. 对于群 (3), $A=\langle b^p,a_1,a_2\rangle$. 通过计算, $\frac{A}{\Phi(A)}=\frac{A}{\langle b^{p^2},a_1^p\rangle}$, $\frac{|A|}{|\Phi(A)|}=\frac{p^{n-1}}{p^{n-4}}=p^3$. 故 $\mathrm{d}(A)=3$. 所以, 我们只要验证类型 (3a) 和 (3b) 的群不同构. 注意到 $G_3=\langle a_1^p\rangle$ 是 G 的特征子群. 若否, 这两种群同构. 在群 (3a) 中, 令 $a_1'=a_1^sb^{tp^{n-4}}a_2^u$, $b'=b^va_1^ra_2^w$ 和 $a_2'=[a_1',b']$, 其中 s,t,u,r,v,w 是合适的非负整数而且 $p\nmid s$, $p\nmid v$. 则 a_1', b', a_2' 满足群 (3b) 的定义关系. 特别地, $[a_2',b']=a_1'^{tp}$. 计算可得, $[a_2',b']=[a_1',b',b']=[a_1^sb^{tp^{n-4}}a_2^u,b^va_1^ra_2^w,b^va_1^ra_2^w]=[a_1^s,b^v,b^v]=[a_1,b,b]^{sv^2}=a_1^{sv^2p}=a_1'^{v^2p}$.

因此, $t = v^2$, 矛盾. □

§4.4 三元生成有交换极大子群的 $\mathcal{A}_2$ 群的分类

本节我们决定三元生成有交换极大子群的 $\mathcal{A}_2$ 群.

定理 4.4.1. 设 G 是三元生成的 $\mathcal{A}_2$ 群且有一个交换的极大子群. 则 $c(G)=2$, $|G'|\leqslant p^2$, $\exp(G')=p$ 且 G 是以下互不同构的群之一:

(1) $\langle a,b\rangle\times C_p$, 其中 $\langle a,b\rangle$ 是亚循环极小非交换 p 群且 $|\langle a,b\rangle|\geqslant p^4$; $(|G|=p^{m+n+1})$

(2) $\langle a,b\rangle\times C_p$, 其中 $\langle a,b\rangle$ 是非亚循环极小非交换 p 群且 $|\langle a,b\rangle|\geqslant p^4$, 即 $G=\langle a,b,d \mid a^{p^m}=b^{p^n}=c^p=d^p=1,[a,b]=c,[c,a]=[c,b]=[d,a]=[d,b]=1\rangle$ 其中 $m\geqslant n$, $n\geqslant 2$; $(|G|=p^{m+n+2})$

(3) $\langle a,b\rangle * C_{p^2}$, 其中 $\langle a,b\rangle$ 是非亚循环非交换 p 群且 $|\langle a,b\rangle|\geqslant p^4$, 即 $G=\langle a,b,d \mid a^{p^m}=b^{p^n}=d^{p^2}=1,[a,b]=d^p,[d,a]=[d,b]=1\rangle$, 其中 $m\geqslant n$, $n\geqslant 2$; $(|G|=p^{m+n+2})$

(4) $p=2$, $G=\langle a,b,c \mid a^4=b^4=1,c^2=a^2b^2,[a,b]=b^2,[c,a]=a^2,[c,b]=1\rangle$; $(|G|=2^5)$

(5) $\langle a,b\rangle\rtimes C_p$, 其中 $\langle a,b\rangle$ 是亚循环极小非交换 p 群, 即 $G=\langle a,b,d \mid a^{p^m}=b^{p^2}=d^p=1,[a,b]=a^{p^{m-1}},[d,a]=b^p,[d,b]=1\rangle$, 若 $p=2$, $m\geqslant 3$; $(|G|=p^{m+3})$

(6) $\langle a,b,d \mid a^{p^m}=b^{p^2}=d^{p^2}=1,[a,b]=d^p,[d,a]=b^{jp},[d,b]=1\rangle$, $(j,p)=1$, $p>2$. j 是一个固定的模 p 的平方非剩余且满足 $-4j$ 是模 p 的平方非剩余; $(|G|=p^{m+4})$

(7) $\langle a,b,d \mid a^{p^m}=b^{p^2}=d^{p^2}=1,[a,b]=d^p,[d,a]=b^{jp}d^p,[d,b]=1\rangle$, $(j,p)=1$ 且满足 $1-4j$ 是模 p 的平方非剩余. 满足这个定义关系的群有 $\frac{p-1}{2}$ 个. 若 $p=2$, $j=1$. $(|G|=p^{m+4})$

证明 设 K 是 G 的非交换的真子群. 则 K 是 G 的极大子群且是内交换群. 根据定理 2.1.4, $|K'|=p$, $\mathrm{d}(K)=2$ 和 $\mathrm{Z}(K)=\Phi(K)$. 由

$\Phi(K) \leqslant \Phi(G)$ 和 $\mathrm{d}(G)=3$, 我们有 $\Phi(K)=\Phi(G)$. 设 A 是 G 的交换极大子群. $\mathrm{Z}(K) \leqslant \mathrm{Z}(G)$. 因为 $G' \leqslant \Phi(G)=\Phi(K)=\mathrm{Z}(K) \leqslant \mathrm{Z}(G)$, 所以 $c(G)=2$.

假设 $G=\langle a,b,d\rangle$. 因为 $c(G)=2$, 所以 $G'=\langle [a,b],[a,d],[b,d],G_3\rangle = \langle [a,b],[a,d],[b,d]\rangle$. 又 $o([a,b]) \leqslant p$, $o([a,d]) \leqslant p$, $o([b,d]) \leqslant p$, 故 $\exp G' = p$.

由于 $|K'|=p$, 根据引理 4.3.1, $|G'| = \frac{p|K'||Z(K)|}{|Z(G)|} = \frac{p^2|Z(K)|}{|Z(G)|}$. 因此有两种情况: $|G'|=p$ 和 $|\mathrm{Z}(G)/\mathrm{Z}(K)|=p$, 或者 $|G'|=p^2$ 和 $\mathrm{Z}(K)=\mathrm{Z}(G)$. 故 $|G'| \leqslant p^2$.

情形I: $|G'|=p$ 和 $|\mathrm{Z}(G)/\mathrm{Z}(K)|=p$. 由于 $|G| \geqslant p^5$, 根据定理 3.2.2, G 不是内亚循环群.

子情形(i): G 的所有非交换极大子群都亚循环. 根据定理 2.1.6, 假设

$$K=\langle a,b \mid a^{p^m}=b^{p^n}=1, [a,b]=a^{p^{m-1}}\rangle,\ m \geqslant 2, \tag{3.1}$$

是一个极大子群. $G'=\langle a^{p^{m-1}}\rangle$. 由 G 不是极小非亚循环群可知, G 有一个交换的极大子群 A 满足 $d(A) \geqslant 3$. 设 $d \in \Omega_1(A)\backslash K$. 则 $d^p=1$ 且 $G=\langle a,b,d\rangle$.

我们断言 $[b,d]=1$. 设 $M=\langle a^p,b,d\rangle$. 若 $m \geqslant 3$, 则 $M/\Phi(M) = \frac{\langle a^p,b,d\rangle}{\langle a^{p^2},b^p\rangle}$ 的阶为 p^3. 因此 $M'=1$, $[b,d]=1$. 若 $m=2$, 则 $n \geqslant 2$ 且 $\Omega_1(M)=\langle a^p, b^{p^{n-1}}, d\rangle$. 因为 $d(\Omega_1(M))=3$, 所以 M 非亚循环. 故 $M'=1$, $[b,d]=1$. 若 $[d,a] \neq 1$, 由 $|\langle d,a\rangle| = p^{m+1} = |K|$, 有 $n=1$. 设 $[d,a]=a^{jp^{m-1}}$ 且 $d_1=db^j$. 则 $[d_1,a]=1, [d_1,b]=1$, $d_1^p=(db^j)^p=d^pb_j^p=1$. 这样, $G=\langle a,b,d_1\rangle$ 同构于类型 (1).

子情形(ii): G 有一个非亚循环的极小非交换的极大子群. 设

$$K=\langle a,b \mid a^{p^m}=b^{p^n}=c^p=1, [a,b]=c, [c,a]=[c,b]=1\rangle, \tag{3.2}$$

是 G 的极大子群. 则 $G' = K' = \langle c \rangle$. 由 K/G' 的型不变量是 (p^m, p^n), 那么 G/G' 的型不变量是 (p^m, p^n, p). 因此存在 $d \in G \setminus K$ 满足 $G = \langle a, b, d \rangle$ 且 $d^p \in G'$. 假设 $d^p = c^k$.

若 $[d, a] \neq 1$, 则 $\langle d, a \rangle$ 是 G 的极大子群. 由 $|\langle d, a \rangle| = p^{m+2} = |K| = p^{m+n+1}$, 得到 $n = 1$. 这样, $|\langle d, b \rangle| \leqslant p^3 < |K|$, 因而有 $[d, b] = 1$. 设 $[d, a] = c^j$, $d_1 = db^j$. $[d_1, a] = 1$, $[d_1, b] = 1$ 以及 $d_1^p = d^p$. 同理, 可以假设 $[d, b] = 1$. 因此, 我们可以假设 $d \in Z(G)$.

若 $d^p = 1$, G 是类型 (2).

若 $d^p = c^k$, 其中 $(k, p) = 1$, 令 $d_1 = d^{k'}$, 其中 $kk' \equiv 1 \pmod p$. 则 $d_1^p = c$. 用 d_1 代替 d, G 是类型 (3).

接下来证明类型 (1), (2), (3) 的群是 $\mathcal{A}_2$ 群. $A = \langle d, a, \Phi(G) \rangle$, $A_i = \langle d, ba^i, \Phi(G) \rangle$, 其中 $0 \leqslant i \leqslant p-1$, 是 G 的 $p+1$ 个交换极大子群, A/G' 和 A_i/G' 的型不变量分别是 (p^m, p^{n-1}, p), (p^{m-1}, p^n, p). 因为 G/G' 的型不变量是 (p^m, p^n, p), 所以它有 $p+1$ 个三元生成的极大子群. 设 K 是 G 的非交换的极大子群. 则 $K/K' = K/G'$ 的型不变量是 (p^m, p^n). 这样, $d(K) = 2$. 根据定理 2.1.4, K 是内交换群. 因此, $G \in \mathcal{A}_2$.

证明类型 (1)–(3) 的群互不同构. 我们注意到群 (2) 有一个四元生成的交换极大子群, 而群 (1) 或 (3), 交换极大子群的生成元个数至多为三.

对于类型 (1), $G' = \langle a^{p^{m-1}} \rangle$ 和 $\mho_2(G) = \langle a^{p^2}, b^{p^2} \rangle$. 当 $m \geqslant 3$ 时, $G' \leqslant \mho_2(G)$; 当 $m = 2$ 时, $G' \nleqslant \mho_2(G)$. 对于类型 (3), $G' = \langle d^p \rangle$ 和 $\mho_2(G) = \langle a^{p^2}, b^{p^2} \rangle$. 则 $G' \nleqslant \mho_2(G)$. 这样, 当 $m \geqslant 3$ 时, 群 (1) 与群 (3) 互不同构. 我们仅需要证明当 $m = 2$ 时, 群 (1) 与群 (3) 互不同构. 反之, 假设类型 (1) 的群 $G(m = 2)$ 同构于类型 (3) 的群 G_1(参数为 m_1, n_1). $Z(G)$ 的型不变量是 (p^{n-1}, p, p), $Z(G_1)$ 的型不变量是 $(p^{m_1-1}, p^{n_1-1}, p^2)$. 因此 $m_1 = n_1 = 2$ 且 $n = 3$. 故 $\exp(G) = p^3$,

$\exp(G_1)=p^2$. 矛盾.

情形 II: $|G'|=p^2$ 和 $Z(K)=Z(G)$. 则 G 的交换的极大子群 A 唯一. 反之, 若 G 有两个不同的交换极大子群 A 和 H, 那么 $G=\langle A,H\rangle$ 且 $A\cap H=Z(G)$. 又 $|A:A\cap H|=p$, 所以 $|G:Z(G)|=|G:Z(K)|=p^2$, 矛盾于 $|G:Z(K)|=p^3$.

子情形(i): $d(A)\geqslant 3$ 且 G 有一个非交换极大子群 K, K 是亚循环群. 因为 $\exp(G')=p$, 所以 $G'=\Omega_1(\Phi(G))=\Omega_1(\Phi(K))=\langle a^{p^{m-1}},b^{p^{n-1}}\rangle$. 因此 $n\geqslant 2$. 设 $d\in\Omega_1(A)\backslash K$. 则 $d^p=1$, $G=\langle a,b,d\rangle$. 因为 $d\notin Z(G)=Z(K)$, 所以 $[d,a]\neq 1$ 或者 $[d,b]\neq 1$. 若 $[d,a]\neq 1$, 则 $\langle d,a\rangle$ 是非交换的极大子群. 由 $|\langle d,a\rangle|\leqslant p^{m+2}$, $n=2$. 同理, 若 $[d,b]\neq 1$, 则 $m=2$. 故 $\min\{m,n\}=2$.

假设 $m>2$. 则 $[d,b]=1$ 且 $[d,a]\neq 1$. 设 $[d,a]=b^{ip}a^{jp^{m-1}}$. 由于 $|G'|=p^2$, $p\nmid i$. 令 $b_1=(b^ia^{jp^{m-2}})^{i'}$ 其中 $ii'\equiv 1 \pmod p$ 且 $d_1=d^{i'}$, 有 $[d_1,b_1]=1$, $[d_1,a]=b_1^p$ 和 $[a,b_1]=a^{p^{m-1}}$. 则 $G=\langle a,b_1,d_1\rangle$ 同构于类型 (5).

其次假设 $m=2$ 和 $n>2$. 则 $[d,a]=1$ 和 $[d,b]\neq 1$. 设 $[d,b]=b^{kp^{n-1}}a^{lp}$. 由于 $|G'|=p^2$, $p\nmid k$. 不失一般性, 设 $[d,b]=b^{p^{n-1}}a^{lp}$. 选择合适的 u 使得 $[da^u,b]=b^{p^{n-1}}$. 设 $a_1=b$, $b_1=da^u$. 用 $M=\langle a_1,b_1\rangle$ 代替 K, 我们把这种情况归结到前面一种情况. G 同构于类型 (5).

最后, 假设 $m=n=2$. 我们可以设 $[d,a]\neq 1$. 由 $A\cap K>\Phi(K)$, 存在元素 $a^xb^y\in A\setminus\Phi(K)$ 满足 $[d,a^xb^y]=1$, 其中 $p\nmid y$. 设 $b_1=a^xb^y$. 则 $K=\langle a,b_1\rangle$, $[d,b_1]=1$. a 和 b_1 与 a 和 b 满足相同的定义关系. (用 a 的适当方幂代替 a). 令 $[d,a]=b_1^{ip}a^{jp}$. 若 $p>2$ 且 $p\nmid j$, 令 $b_2=b_1^ia^j$. 则 $b_2^p=[d,a]$ 和 $[d,b_2]=[d,a^j]=b_2^{jp}$. 故 $\langle d,b_2\rangle$ 非交换且阶为 p^3, 即指数为 p^2 的非交换群, 矛盾. 不失一般性设 $[d,a]=b^p$. 这样, G 是类型 (5). 若 $p=2$, 得到 (a) $[d,a]=b^2$ 和 (b) $[d,a]=b^2a^2$. 因为 $(ab)^2=a^2b^2[b,a]=b^2$, 所以, 对于 (a) $\langle ab,d\rangle\cong D_8$; 对于 (b),

$\langle ab, bd\rangle \cong Q_8$. $\langle ab, d\rangle$ 和 $\langle ab, bd\rangle$ 都是指数为 4 的非交换群, 矛盾.

接下来证明类型 (5) 的群是 $\mathcal{A}_2$ 群.

由 G 三元生成, G 有 p^2+p+1 个极大子群. K 和交换群 $A=\langle a^p, b, d\rangle(\mathrm{d}(A)=3)$ 是 G 的极大子群. 设 $K_j=\langle b, da^j\rangle$ $((j,p)=1)$, $K_i=\langle ab^i, d\rangle$, $K_{ij}=\langle ab^i, db^j\rangle$ $((j,p)=1)$. 下面将要证明 K_i, K_j, K_{ij} 都包含 $\Phi(G)=\langle a^p, b^p\rangle$.

对于 $K_j=\langle b, da^j\rangle$(其中 $(j,p)=1$), 因为 $(da^j)^p=d^pa^{jp}[d,a^{-j}]^{\binom{p}{2}}=d^pa^{jp}b^{-jp\binom{p}{2}}=a^{jp}b^{-jp\binom{p}{2}}$ 和 $[b, da^j]=[b,a^j]=a^{-jp^m}$, 所以 $\Phi(K_j)=\Phi(G)=\langle a^p, b^p\rangle$. 因此 $K_j=\langle b, da^j\rangle$ 是极大子群.

对于 $K_i=\langle ab^i, d\rangle$, 因为 $(ab^i)^p=a^pb^{ip}a^{-ip^m\binom{p}{2}}$ 和 $[ab^i, d]=b^{-p}$, 所以 $\Phi(K_i)=\Phi(G)=\langle a^p, b^p\rangle$. 因此 $K_i=\langle ab^i, d\rangle$ 是极大子群.

对于 $K_{ij}=\langle ab^i, db^j\rangle$, (其中 $(j,p)=1$), 因为 $(ab^i)^p=a^pb^{ip}a^{-ip^m\binom{p}{2}}$, $(db^j)^p=b^{jp}$ 和 $[ab^i, db^j]=b^{-p}a^{jp^m}$, 所以 $\Phi(K_{ij})=\Phi(G)=\langle a^p, b^p\rangle$. 因此 $K_{ij}=\langle ab^i, db^j\rangle$ 是极大子群.

以上这些非交换群都是二元生成, 因为 $c(G)=2$, 所以这些群都是 $\mathcal{A}_1$ 群. 故, G 是 $\mathcal{A}_2$ 群.

子情形(ii): $d(A)\geqslant 3$ 且 G 的非交换的极大子群都非亚循环. 根据定理 2.1.6, 设

$$K=\langle a, b \mid a^{p^m}=b^{p^n}=c^p=1, [a,b]=c, [c,a]=[c,b]=1\rangle$$

是极大子群并且 $m\geqslant n$. 因为 $|G|\geqslant p^5$, $m\geq 2$. 更多地, $\mathrm{Z}(G)=\mathrm{Z}(K)=\langle a^p, b^p, c\rangle < A\cap K$ 和 $G'\leq \Omega_1(\Phi(G))=\Omega_1(\Phi(K))=\langle a^{p^{m-1}}, b^{p^{n-1}}, c\rangle$.

$\forall g\in A\setminus K$, 我们断言 $o(g)>p$. 因而 $\Omega_1(A)\leqslant K$, $\mathrm{d}(A)=3$. 反之, $o(g)=p$. 因为 $g\notin \mathrm{Z}(G)=\mathrm{Z}(K)$, 所以 $[g,a]\neq 1$ 或者 $[g,b]\neq 1$. 若 $[g,b]\neq 1$, 则 $\langle g, b\rangle$ 的阶为 p^{n+2}, $|G|=p^{n+3}$. 这样, $m=1$, 矛盾. 故我们有 $[g,a]\neq 1$, 以及 $n=1$. 因此 $b\notin \Phi(G)=\Phi(K)$, $G'=\langle a^{p^{m-1}}, c\rangle$. 由 $a\notin A$, 根据定理 2.1.3, 存在 $e\in A$ 满足 $[e,a]=a^{p^{m-1}}$. 这样, $\langle e, a\rangle$ 是非交换群并且亚循环. 矛盾. 由 $d(A)=d(\Omega_1(A))\leqslant d(\Omega_1(K))=3$. 推得

$d(A)=3$. 因此, $|\Phi(G):\Phi(A)|=p$, $G'\cap\Phi(A)\neq 1$. 若否, $G'\cap\Phi(A)=1$. 则 $|G'\Phi(A)|=p^{m+n}>|\Phi(G)|=p^{m+n-1}$, 矛盾.

我们断言当 $m>n$ 时, $a\notin A$. 若否, $a\in A$ 也即 $b\notin A$. 既然 $d(A)=3$, 那么可设 $A=\langle a\rangle\times\langle z_1\rangle\times\langle z_2\rangle$. 因为 $|A|=|K|=p^{m+n+1}$, 所以 $o(z_1)<p^m$ 且 $o(z_2)<p^m$. 这样, $|\langle z_1,b\rangle|<|K|$, $|\langle z_2,b\rangle|<|K|$, 而且也就有 $[z_1,b]=[z_2,b]=1$. 根据定理理 2.1.3, $G'=[A,b]=\langle[a,b]\rangle$. 故 $|G'|=p$, 矛盾.

设 $m=n$ 且 $a\in A$. 则 $b\notin A$. 设 $a_1=b, b_1=a, c_1=c^{-1}$, a_1,b_1,c_1 与 a,b,c 有相同关系, $a_1\notin A$. 用 a_1 代替 a. 但形式上我们仍用 a 来表示.

取 $d\in A\backslash K$ 满足 $d^p\in G'\cap\Phi(A)$. 根据定理 2.1.3, 存在元 $f\in A$ 满足 $[f,a]=d^p$. $\langle a,f\rangle$ 是 G 的一个非交换的极大子群, 非亚循环. 由于 $\exp(G)=\exp(K)=p^m$, $\langle a,f\rangle$ 同构于 K. 用 b 代替 f, 假设 $G=\langle a,b,d\rangle$, 定义关系是 $a^{p^m}=b^{p^n}=d^{p^2}=1, [a,b]=d^p, [d^p,a]=[d^p,b]=1$. 因为 $\langle a,d\rangle$ 和 $\langle a,b\rangle$ 都是 G 的极大子群且都非亚循环 $\mathcal{A}_1$ 群, 所以它们有相同的阶. 故 $n=2$.

接下来考虑 G'. 由于 $G'\neq\langle a^{p^{m-1}},d^p\rangle$. 设 $G'=\langle a^{ip^{m-1}}b^p,d^p\rangle$(对于某些 i). 不失一般性, 假设 $G'=\langle b^p,d^p\rangle$. (若 $(i,p)=1$, 用 $a^{ip^{m-2}}b$ 代替 b). 因为 $\langle d\rangle\langle b\rangle\geqslant G'$, $|\langle d\rangle\langle b\rangle|=p^4$, 所以 $[d,b]=1$. 这样, 我们得到 $G\cong G_{(j,k)}=\langle a,b,d\rangle$ 满足下面的定义关系

$$a^{p^m}=b^{p^2}=d^{p^2}=1, [a,b]=d^p, [d,b]=1, [d,a]=b^{jp}d^{kp}, \qquad (*)$$

$p\nmid j$.

若 $p=2$, 断言 $j=k=1$. 也就是说, $[d,a]=b^2d^2$, 即 G 是类型 (7)($m\geqslant 2$). 若否, $[d,a]=b^2$. 则 $[bd,a]=b^2d^2=(bd)^2$, 故 $\langle bd,a\rangle$ 是指数为 4 的非交换群, 矛盾.

以下, 我们决定满足子情形 (ii) 的群 $(*)$ 是 $\mathcal{A}_2$ 群的充分必要条件, 也就是说, 任一个非交换的极大子群都是非亚循环的内交换群. G 的

非交换的极大子群如下: $K_{xy}=\langle ab^x,db^y,\Phi(G)\rangle$ 和 $K_z=\langle ad^z,b,\Phi(G)\rangle$, 其中 $0\leqslant x,y,z\leqslant p-1$. K_z 是内交换群且非亚循环. 对于 K_{xy} 来说, 因为 $[ab^x,db^y]=[a,db^y]=b^{-jp}d^{(y-k)p}$, 所以 K_{xy} 是内交换群当且仅当 $d(K_{xy})=2$, 也就是说, $\Phi(K_{xy})=\Phi(G)=\langle a^p,b^p,d^p\rangle$. 注意到 $\Phi(K_{xy})=\langle a^pb^{xp},d^pb^{yp},[ab^x,db^y]\rangle$. 故 $b^{-jp}d^{(y-k)p}\notin\langle db^y\rangle$ 即 $\begin{vmatrix}-j & y-k\\ y & 1\end{vmatrix}\neq 0\ (\mathrm{mod}\ p)$, $\forall y$, 因而 $-j-y(y-k)\not\equiv 0(\mathrm{mod}\ p)$, $\forall y$, 等价于 k^2-4j 是模 p 的平方非剩余. 反过来, 若 k^2-4j 是模 p 的平方非剩余, 则 K_{xy} 是非亚循环 $\mathcal{A}_1$ 群.

下面决定 $(*)$ 中互不同构的类型. 假设 $p>2$. $a'=a^xb^yd^z$, $b'=b^rd^sa^t$, $d'=b^ud^va^w$, 其中 x,y,z,r,s,t,u,v,w 是合适的非负整数. 设 a',b',d' 生成 G, 满足 $(*)$ 中除了最后一个关系以外的定义关系, 还满足 $[d',a']=b'^{j'p}d'^{k'p}$. 换句话说, 就是假设了 $G_{(j,k)}\cong G_{(j',k')}$. 由 $G'=\langle b'^p,d'^p\rangle=\langle b^p,d^p\rangle$ 以及 $b'^p=b^{rp}d^{sp}a^{tp}$ 和 $d'^p=b^{up}d^{vp}a^{wp}$, 通过计算, 我们有 $p^{m-1}\mid t$, $p^{m-1}\mid w$. 由于 $G=\langle a',b',d'\rangle$, 所以 $p\nmid x$ 且 $p\nmid rv-us$. 由

$$[a',b']=d'^p=b^{up}d^{vp}$$

和

$$\begin{aligned}[a',b'] &= [a^xb^yd^z,b^rd^sa^t]=[a^x,b^rd^s][b^yd^z,a^t]\\ &= [a,b]^{xr}[a,d]^{xs}=d^{xrp}(b^{jp}d^{kp})^{-xs}=b^{-xsjp}d^{(xr-xsk)p}\end{aligned}$$

可得

$$u\equiv -xjs(\mathrm{mod}\ p),v\equiv x(r-ks)(\mathrm{mod}\ p). \tag{1}$$

由

$$[d',a']=b'^{j'p}d'^{k'p}=(b^{rp}d^{sp})^{j'}(b^{up}d^{vp})^{k'}=b^{p(rj'+uk')}d^{p(sj'+vk')}$$

和

$$\begin{aligned}[d',a'] &= [b^u d^v a^w, a^x b^y d^z] = [b^u d^v, a^x b^y d^z] = [b^u d^v, a^x] \\ &= [b,a]^{ux}[d,a]^{vx} = d^{-uxp}(b^{jp}d^{kp})^{vx} = b^{jvxp}d^{(kvx-ux)p}\end{aligned}$$

可得

$$\begin{cases} rj' + uk' \equiv jvx \pmod p \\ sj' + vk' \equiv kvx - ux \pmod p \end{cases} \quad (2)$$

由 (2) 解得,

$$j' \equiv \frac{\begin{vmatrix} jvx & u \\ -ux+kvx & v \end{vmatrix}}{\begin{vmatrix} r & u \\ s & v \end{vmatrix}} \pmod p$$

以及

$$k' \equiv \frac{\begin{vmatrix} r & jvx \\ s & -ux+kvx \end{vmatrix}}{\begin{vmatrix} r & u \\ s & v \end{vmatrix}} \pmod p.$$

把 (1) 代入, 有

$$\begin{aligned} j' &\equiv \tfrac{jv^2x-ux(-u+kv)}{rv-us} \pmod p \\ &\equiv \tfrac{jx^2(r-sk)^2x+x^2sj[xsj+kx(r-sk)]}{rx(r-sk)+xs^2j} \\ &= \tfrac{x^2\{j(r-sk)^2+sj[sj+k(r-sk)]\}}{r(r-sk)+s^2j} \\ &= \tfrac{x^2(-sjkr+s^2j^2+jr^2)}{r(r-sk)+s^2j} \\ &= \tfrac{x^2j(-skr+s^2j+r^2)}{r(r-sk)+s^2j} = x^2j \end{aligned}$$

和

$$\begin{aligned}
k' &\equiv \frac{r(-ux+kvx)-jvxs}{rv-us} \qquad\qquad (\mathrm{mod}\ p)\\
&= \frac{-rux+vx(kr-js)}{rv-us}\\
&\equiv \frac{-r(-x^2sj)+x^2(r-sk)(kr-js)}{rx(r-sk)+xs^2j}\\
&= \frac{x[rsj+(r-sk)(kr-js)]}{r(r-sk)+s^2j}\\
&= \frac{x(kr^2-k^2sr+s^2kj)}{r^2-rsk+s^2j}\\
&= \frac{kx(r^2-ksr+s^2j)}{r^2-rsk+s^2j}\\
&= kx
\end{aligned}$$

故

$$j' \equiv jx^2 (\mathrm{mod}\ p) \quad 和 \quad k' \equiv kx (\mathrm{mod}\ p). \tag{$**$}$$

这就证明了 $G_{(j,k)} \cong G_{(j',k')}$ 当且仅当 $(**)$ 成立. 若 $(k', p) = 1$, 令 $x = k'$, 有 $k = 1$, $1 - 4j$ 是模 p 的平方非剩余且 G 是类型 (7)($m \geqslant 2$). 若 $p \mid k'$, 选择合适的 x, 有 $j = -\nu$ 且 G 是类型 (6)($m \geqslant 2$). 以上推导过程也证明了群 (6), (7)($m \geqslant 2$) 是互不同构的 $\mathcal{A}_2$ 群.

子情形(iii): $d(A) = 2$. 由 $\mathrm{d}(G) = 3$, 有 $\Phi(A) = \Phi(G)$. 在此情形下, 因为 G 的所有极大子群都是二元生成的, 所以 G/G' 没有三元生成的真子群, 因此它的型不变量是 (p, p, p). 故 $|G| = p^5$, $G' = \Phi(G)$.

(iiia) 若 G 的所有极大子群都亚循环, 根据定理 3.2.2, G 是类型 (4). 下面证明类型 (4) 是 $\mathcal{A}_2$ 群.

由 $d(G) = 3$, G 有 $2^2 + 2 + 1$ 个极大子群. $\mathrm{Z}(G) = \Phi(G) = \langle a^2, b^2\rangle$. 设 $L_1 = \langle\langle\Phi(G), a, c\rangle$, $L_2 = \langle\langle\Phi(G), a, b\rangle$, $L_3 = \langle\Phi(G), ab, c\rangle$, $L_4 = \langle\Phi(G), ac, bc\rangle$, $L_5 = \langle\Phi(G), a, bc\rangle$, $L_6 = \langle\Phi(G), ac, b\rangle$, $L_7 = \langle\Phi(G), b, c\rangle$. 则 G 的所有极大子群是 $L_i (i = 1, 2, \ldots, 7)$. 因为 $L_1 = \langle a, c\rangle$ 和 $L_2 = \langle a, b\rangle$ 是亚循环的内交换群以及 $L_7 = \langle b, c\rangle$ 是交换群, 所以 G 是 $\mathcal{A}_2$ 群当且仅当 $|L_i'| = 2$, $d(L_i) = 2$, 其中 $i = 3, 4, 5, 6$, (也即 $|L_i'| = 2$ 和 $|\Phi(L_i)| = 4$).

对于 L_3, $(ab)^2 = b^2$, $[ab, c] = a^2 = (ab)^2c^2$. 因为 $|L_3'| = 2$ 和 $|\Phi(L_3)| = 4$, 所以 $L_3 = \langle ab, c\rangle$ 是内交换群.

对于 L_4, $(ac)^2 = c^2 = a^2b^2$, $(bc)^2 = b^2c^2 = a^2$, $[ac, bc] = a^2b^2 = (ac)^2$. 因为 $|L_4'| = 2$ 和 $|\Phi(L_4)| = 4$, 所以 $L_4 = \langle ac, bc\rangle$ 是内交换群.

对于 L_5, $[a, bc] = a^2b^2 = (abc)^2$. 因为 $|L_5'| = 2$ 和 $|\Phi(L_5)| = 4$, 所以 $L_5 = \langle a, bc\rangle$ 是内交换群.

对于 L_6, $[ac, b] = b^2$. 因为 $|L_6'| = 2$ 和 $|\Phi(L_6)| = 4$, 所以 $L_6 = \langle a, bc\rangle$ 是内交换群.

(iiib) G 有一个非亚循环的 $\mathcal{A}_1$ 群,

$$K = \langle a, b, c \mid a^p = b^{p^2} = c^p = 1, [a, b] = c, [c, a] = [c, b] = 1\rangle.$$

K 的所有极大子群分别是: $\langle\Phi(G), a\rangle = \langle b^p, c, a\rangle$ 和 $\langle\Phi(G), ba^s\rangle = \langle c, ba^s\rangle$, 其中 $s = 0, 1, \ldots, p-1$. 由 $d(A) = 2$, 通过令 $b' = ba^s$, 我们可以假设 $A \cap K = \langle b', c\rangle$. 再用 b 代替 b', $A \cap K = \langle b, c\rangle$.

设 $p = 2$. 由 $a \notin A$ 和 $b^2c \in \Phi(G) = G'$, 根据定理 2.1.3, 存在元 $d \in A$ 满足 $[d, a] = b^2c$. 因为 $c \in G' = \Phi(A)$, 所以 $A = \langle b, d\rangle$, $d^4 = 1$. 故有 $G = \langle a, b, d\rangle$. 又因为 $\langle d, a\rangle$ 非交换, 从而 $|\langle d, a\rangle| = 2^4$. 这样, $[d, a] \neq d^2$. 若否, $\langle d, a\rangle$ 是 2^3 阶非交换群. 因此 $c \neq b^2d^2$, $c = d^2$. 所以 G 是类型 (7)($m = 1$).

若 $p > 2$, 取 $d \in A \setminus K$. 则 $G = \langle a, b, d\rangle$. 因为 $A \cap K = \langle b, c\rangle$, 所以 $[b, d] = 1$, $A = \langle b, d, c\rangle$. 因为 $\mathrm{d}(A) = 2$, 所以 $\Phi(A) = \Phi(G)$, 因此 $c \in \Phi(A)$. 故 $A = \langle b, d\rangle$, $d^p \notin \langle b\rangle$. 不失一般性, 我们可以假设 $d^p = c$. 因为 $|G'| = p^2$ 和 $G' \leqslant \Phi(G)$, 所以 $G' = \langle b^p, d^p\rangle$. 故,

$$G = \langle a, b, d \mid a^p = b^{p^2} = d^{p^2} = 1, [a, b] = d^p, [d, b] = 1, [d, a] = b^{jp}d^{kp}\rangle,$$

且 $p \nmid j$.

同于情形 (ii)的证明和计算相同, G 是类型 (6)($m = 1$) 或 (7)($m = 1$), 并且不同的参数确定不同的群, 极大子群除了 A, 其余的都是 $\mathcal{A}_1$ 群.

下面证明群 (4), (5), (6), (7) 互不同构. 群 (4) 是 2^5 阶群并且极大子群都亚循环, 类型 (5) 的阶 $\geqslant 2^6$, 群 (7) 有一个非亚循环的极大子

群 $\langle a,b\rangle$. 故群 (4) 与 (5), (7) 不同构. 考虑群 (5), (6), (7), 已经知道群 (6) 与 (7) 不同构.. 对于群 (5), $|G|=p^{m+3}$, $\exp(G)=p^m$; 对于群 (6) 或 (7), $|G|=p^{m+4}$, $\exp(G)=p^m$ 或 $p^2(m=1)$. 我们只需要验证阶是 p^5 的情况. 对于群 (5), $m=2$ 且有唯一的三元生成的交换极大子群 $\langle b,d,a^p\rangle$; 对于群 (6) 或 (7), $m=1$ 且有唯一的二元生成的交换极大子群 $\langle b,d\rangle$. 所以群 (5) 与群 (6), (7) 都不同构.

下面需要用到一个定理.

定理 4.4.2. ([18, 定理3.1]) 设 G 是有限 p- 群 $(p>2)$ 且 $d(G)>2$. 若对于 G 的极大子群 H 都有 $d(H)\leqslant 2$. 则 G 是以下类型的群之一:

(1) p^3 阶初等交换群;

(2) p^4 阶群, $G=\langle a,b,d \mid a^p=b^p=d^{p^2}=1,[a,b]=d^p,[d,a]=[d,b]=1\rangle$;

(3) 幂零类为 2 的 p^5 阶群, 定义关系如下: $G=\langle a,b,c,x,y \mid [a,b]=x,[a,c]=y,[b,c]=[a,x]=[a,y]=[b,x]=[b,y]=1,a^p=x^p=y^p=1,b^p=x^\alpha y^\beta,c^p=x^\gamma y^\delta\rangle$ 其中 $0\leqslant\alpha,\beta,\gamma,\delta\leqslant p-1$ 且 $4\beta\gamma+(\delta-\alpha)^2$ 是模 p 的平方非剩余. 当参数取不同的值时, 可以决定 $\frac{1}{2}(p+1)$ 个互不同构的群.

定理 4.4.3. 当参数取不同的值, 定理 4.4.1 中的类型(7) 可以决定 $\frac{p-1}{2}$ 种互不同构的群. 我们只需要证明定理 4.4.1 中的类型(6)$(m=1)$ 和(7)$(m=1)$ 的每一种群都同构于定理 4.4.2 中的类型(3)中的某种群以及证明定理 4.4.2 中的类型(3)中的每一种群同构于定理 4.4.1 中的类型(6)$(m=1)$ 或者(7)$(m=1)$ 的某种群. 换句话说, 定理 4.4.1 中的类型(6)$(m=1)$ 和(7)$(m=1)$ 决定的 $\frac{p+1}{2}$ 个群是定理 4.4.2 中的类型(3)中不同参数决定的群的另一种表述形式.

证明 首先证明定理 4.4.1 中的类型(6)$(m=1)$ 和(7)$(m=1)$ 的每一种群同构于定理 4.4.2 中的类型(3)中的某种群.

设 $c = d$, $x = [a, b], y = [a, c]$. 则 $x = c^p, y = b^{-jp}d^{-kp}$ $(k = 0, 1)$, 也有 $y = b^{-jp}x^{-k}$. 因此 $b^p = x^{-kj'}y^{-j'}$, 其中 $jj' \equiv 1(\mathrm{mod}\ p)$.

设 $\alpha = -kj', \beta = -j', \gamma = 1, \delta = 0$. 则 $b^p = x^\alpha y^\beta, c^p = x$. 参数 $\alpha, \beta, \delta, \gamma$ 满足以下关系: $4\beta\gamma + (\delta - \alpha)^2 = 4(-j') + (kj')^2 = -4j' + k^2j'^2 = j'^2(k^2 - 4j)$ 是模 p 的平方非剩余. 我们有

$$G = \langle a, b, d \mid [a, b] = x, [a, c] = y, [b, c] = [a, x] = [a, y] = [b, x] = [b, y] = 1$$

$$a^p = x^p = y^p = 1, b^p = x^\alpha y^\beta, c^p = x^\gamma y^\delta\rangle$$

其中 $4\beta\gamma + (\delta - \alpha)^2$ 是模 p 的平方非剩余.

其次证定理 4.4.2 中的类型(3)中的每一种群同构于定理 4.4.1 中的类型(6)$(m = 1)$ 或者(7)$(m = 1)$ 的某种群.

设 $b_1 = b^\gamma c^\delta$. 则 $[a, b_1] = [a, b^\gamma c^\delta] = [a, b]^\gamma [a, c]^\delta = x^\gamma y^\delta = c^p$, $[c, b_1] = [c, b^\gamma c^\delta] = 1$, $[c, a] = [a, c]^{-1} = y^{-1}$. 令 $[c, a] = b_1^{jp}c^{kp}$. 则 $[c, a] = (b^\gamma c^\delta)^{jp}c^{kp} = b^{\gamma jp}c^{(\delta j + k)p} = x^{\alpha\gamma j + \gamma\delta j + \gamma k}y^{\beta\gamma j + \delta^2 j + \delta k}$.

我们有

$$\begin{cases} \alpha\gamma j + \gamma\delta j + \gamma k = 0 \\ \beta\gamma j + \delta^2 j + \delta k = -1 \end{cases} \text{计算可得:} \begin{cases} -k = \alpha j + \delta j \\ j = (\alpha\delta - \beta\gamma)^{-1} \end{cases}$$

所以

$$\begin{cases} \alpha + \delta = -kj' \\ \alpha\delta = \beta\gamma + j' \end{cases}$$

因此 $(\alpha - \delta)^2 = (\alpha + \delta)^2 - 4\alpha\delta = (-kj')^2 - 4(\beta\gamma + j') = k^2j'^2 - 4\beta\gamma - 4j'$.

因为 $(\alpha - \delta)^2 + 4\beta\gamma = k^2j'^2 - 4j' = j'^2(k^2 - 4j)$ 是模 p 的平方非剩余, 所以 $k^2 - 4j$ 是模 p 的平方非剩余. 令 $d = c$. 则

$$G = \langle a, b_1, d \mid a^p = b_1^{p^2} = d^{p^2} = 1, [a, b_1] = d^p, [d, a] = b_1^{jp}d^{kp}, [d, b_1] = 1\rangle$$

其中 k^2-4j 是模 p 的平方非剩余.

若 $k=0$, 定理 4.4.2 中的类型(3)不同参数决定的群同构于定理 4.4.1 中类型 (6) 的群; 若 $(k,p)=1$, 同构于定理 4.4.1 中类型 (7) 的群. □

§4.5 无交换极大子群的 $\mathcal{A}_2$ 群的分类

我们要用到下面的定理.

定理 4.5.1. ([18, 定理5.1]) 设 G 为 2^n 阶群, 其中 $n\geqslant 5, r\in N^+$, $5\leqslant r\leqslant n$. 若 G 的阶为 2^{r-1} 的子群与阶为 2^r 的子群都是二元生成的, 则 G 为亚循环群.

定理 4.5.2. ([18, 定理4.2]) 设 G 是 p^n 阶群, 其中 p 是奇数, $n\geqslant 6$. 若 G 的所有极大子群都是二元生成的, 则 G 为亚循环群或者 $|G/G_3|=p^3$, 且 $\mho_1(G)=G_3$.

定理 4.5.3. ([19]) 设 G 是极大类 3- 群且 $|G|\geqslant 3^5$, 则 G 非 $\mathcal{A}_2$ 群.

定理 4.5.4. ([19]) 设 G 是 p^m 阶的极大类 p- 群, 其中 $m\leqslant p+1$. 则 $\Phi(G)$ 和 $G/\mathrm{Z}(G)$ 的方次数都为 p.

下面先设 $p=2$.

定理 4.5.5. 设 G 是 2- 群. 假设 G 非亚循环且所有极大子群都是 $\mathcal{A}_1$ 群, 则

$$G=\langle a,b,d \mid a^4=b^4=d^4=1,\ [a,b]=d^2,\ [d,a]=b^2d^2,\ [d,b]=a^2b^2\rangle.$$

证明 若 $\mathrm{d}(G)=2$, 根据定理 4.5.1 可知, G 亚循环. 因此 $\mathrm{d}(G)=3$. 设 K_1 和 K_2 都是 G 的极大子群. 则 $G=\langle K_1,K_2\rangle$, $\Phi(G)=\Phi(K_1)=\Phi(K_2)=\mathrm{Z}(K_1)=\mathrm{Z}(K_2)$. 故 $\Phi(G)\leqslant Z(G)$. 断言 $\Phi(G)=\mathrm{Z}(G)$, $c(G)=$

2. 若否, $\Phi(G) < Z(G)$. 存在元 $g \in Z(G)\backslash\Phi(G)$ 满足 $G = \langle g, a, b\rangle$. 故 $\langle\Phi(G), g, a\rangle$ 是交换极大子群, 矛盾.

由 $c(G) = 2$ 和 $d(G) = 3$ 可得, $\exp(G') = 2$.

考虑 G/G'. 由 G 的极大子群都是二元生成的和 $G' \leqslant \Phi(K_1)$, 有 G/G' 的极大子群都是二元生成的, 从而 G/G' 的型不变量是 $(2, 2, 2)$, 即 $|G/G'| = 2^3$. 因此 $G' = \Phi(G)$. 从而 $\exp(G') = 4$. 又因为 $G' = \Phi(G) = \mathrm{Z}(G) = \Omega_1(Z(G))$, 所以 G 是特殊 2- 群. 又因为 $c(G) = 2$, $\exp(G') = 2$ 以及 $d(G) = 3$, 所以 $|G'| \leqslant 2^3$. 若 $|G'| = 2$, 则 $|G| = 2^4$. 若 $|G'| = 2^2$, 设 $G = \langle a, b, d\rangle$, $G' = \langle e, f\rangle$. 令 $[a, b] = e$ 和 $[a, d] = f \neq e$, 则 $[b, d] = ef$, 从而 $\langle\Phi(G), ab, bd\rangle$ 是 G 的交换极大子群, 矛盾. 因此 G' 是 2^3 阶初等交换群, 那么 $|G| = 2^6$, G 的全部极大子群都非亚循环.

对于 $x, y \in G\backslash G'$ 满足 $xG' \neq yG'$. 因为 $[x, y] \neq 1$, 所以 $\langle x, y\rangle$ 非交换. 又 G 是 $\mathcal{A}_2$ 群, 所以 $\langle x, y\rangle$ 是 G 的极大子群. 由 $\exp(G) = 4$ 可知, $\langle x, y\rangle$ 非亚循环, 并且可设

$$\langle x, y \mid x^{2^2} = y^{2^2} = z^2 = 1, [x, y] = z, [z, x] = [z, y] = 1\rangle.$$

特别地, $x^2 \neq y^2$. 故七个 (模 $\Phi(G)$) 的不同元素有不同的平方. 因此 G' 中的任意元都可以表示成另一个元平方的形式.

设

$$K = \langle a, b \mid a^{2^2} = b^{2^2} = c^2 = 1, [a, b] = c, [c, a] = [c, b] = 1\rangle$$

是 G 的极大子群. 取 $d \in G\backslash K$ 满足 $d^2 = c$. 则 $G = \langle a, b, d\rangle$. 由于 $[d, a] \in G'$, 可令 $[d, a] = b^{2x}a^{2i}d^{2j}$, 其中 $x, i, j = 0$ 或者 1. 则 $x = 1$. 若否, $[d, a] = a^{2i}d^{2j}$. 故 $[db^j, a] = a^{2i}$, $\langle db^j, a\rangle$ 是亚循环的的极大子群, 矛盾. 同样, 可以设 $[d, b] = a^2b^{2k}d^{2l}$, 其中 $k, l = 0$ 或者 1. 由 $\{(ab)^2, (bd)^2, (ad)^2, (abd)^2\} = \{a^2b^2, b^2d^2, a^2d^2, a^2b^2d^2\}$, 得到 i, j, k, l 的四种情形.

对于情形 $i = 0, j = 1, k = 1, l = 0$ 和 $i = 1, j = 0, k = 0, l = 1$ 确定的群是同构的. 对于前一种情形决定的群 $G = \langle a, b, d\rangle$, 令 $a' = ab$. 则

$[a',b]=[ab,b]=d^2,[d,a']=[d,ab]=[d,a][d,b]=a^2d^2=(a^2b^2d^2)b^2=a'^2b^2$, $[d,b]=a^2b^2=(a^2b^2d^2)d^2=a'^2d^2$. 那么, $G=\langle a,b,d\rangle=\langle a',b,d\rangle$ 同构于后一种情形决定的群, 并且同构于定理中的群.

其余两种情形: $i=1,j=0,k=1,l=0$ 和 $i=0,j=1,k=0,l=1$ 是不可能的. 对于前者, 有交换极大子群 $\langle ab,d,\Phi(G)\rangle$; 对于后者, 因为 $(ad)^2=a^2d^2b^2d^2=a^2b^2$, $(bd)^2=b^2d^2a^2d^2=a^2b^2$, 所以 $\langle ad,bd\rangle$ 是指数为 2^2 的非交换群.

为了完成定理的证明, 还需要证 G 是 $\mathcal{A}_2$ 群, 或者等价地, G 的每个极大子群都是 $\mathcal{A}_1$ 群.

$\Phi(G)=G'=Z(G)=\langle a^2,b^2,d^2\rangle$. 设 $L_1=\langle a,d,\Phi(G)\rangle=\langle a,d\rangle$, $L_2=\langle b,d,\Phi(G)\rangle=\langle b,d\rangle$, $L_3=\langle a,b,\Phi(G)\rangle=\langle a,b\rangle$, $L_4=\langle ab,d,\Phi(G)\rangle$, $L_5=\langle ad,b,\Phi(G)\rangle$, $L_6=\langle a,bd,\Phi(G)\rangle$, $L_7=\langle ad,bd,\Phi(G)\rangle$. 则 G 的所有极大子群是 $L_i(i=1,2,\ldots,7)$. 因为 L_1,L_2,L_3 是 $\mathcal{A}_1$ 群, 所以 G 是 $\mathcal{A}_2$ 群当且仅当 $L_t(t=4,5,6,7)$ 是 $\mathcal{A}_1$ 群.

对于 L_4, 因为 $(ab)^2=a^2b^2d^2$, $[ab,d]=a^2d^2$, 所以 $\Phi(L_4)=\langle a^2,b^2,d^2\rangle$ 以及 $L_4'=\langle a^2d^2\rangle$ 的阶是 2. 这样, $L_4=\langle ab,d\rangle$ 是 $\mathcal{A}_1$ 群.

对于 L_5, 因为 $(ad)^2=a^2d^2b^2d^2=a^2b^2$, $[ad,b]=d^2a^2b^2$, 所以 $\Phi(L_5)=\langle a^2,b^2,d^2\rangle$ 以及 $L_5'=\langle a^2b^2d^2\rangle$ 的阶是 2. 这样, $L_5=\langle ad,b\rangle$ 是 $\mathcal{A}_1$ 群.

对于 L_6, 因为 $(bd)^2=b^2d^2a^2b^2=a^2d^2$, $[a,bd]=d^2b^2d^2=b^2$, 所以 $\Phi(L_6)=\langle a^2,b^2,d^2\rangle$ 以及 $L_6'=\langle b^2\rangle$ 的阶是 2. 这样, $L_6=\langle a,bd\rangle$ 是 $\mathcal{A}_1$ 群.

对于 L_7, 因为 $(ad)^2=a^2b^2$, $(bd)^2=a^2d^2$ 和 $[ad,bd]=a^2$, 所以 $\Phi(L_7)=\langle a^2,b^2,d^2\rangle$, 以及 $L_7'=\langle a^2\rangle$ 的阶是 2. 这样, $L_3=\langle ad,bd\rangle$ 是 $\mathcal{A}_1$ 群. □

接下来考虑 $p>2$ 的情况. 首先, 我们给出一个有用的引理.

引理 4.5.6. 设 G 是 p 群, $p>2$. 假设 G 非亚循环且 G 的所有的极大子群都是 $\mathcal{A}_1$ 群. 则 $d(G)=2$, $|G|=p^5$, $c(G)\leqslant 3$, $\exp(G')=p$, $\mho_1(G)\leqslant Z(G)$, 以及

(1) $G=\langle a,b \mid a^{p^2}=b^{p^2}=c^p=1,[a,b]=c,[c,b]=a^{kp},[c,a]=a^{ip}b^{jp}\rangle$, 其中 $(k,p)=1,(j,p)=1$.

(2) 若 $p\geqslant 5$, 则 G 是 $\mathcal{A}_2$ 群当且仅当 i^2+4kj 是模 p 的平方非剩余.

证明 (1) 由于 G 的所有极大子群都是二元生成, 根据定理 4.4.2, $d(G)=2$. 假设 $|G|\geqslant p^6$. 根据定理 4.5.2, 有 $|G/G_3|=p^3$ 和 $\mho_1(G)=G_3$. 设 K 是 G 的极大子群. 则 $K/\mho_1(G)$ 的型不变量是 (p,p). 故 $\mathrm{Z}(K)=\Phi(K)=\mho_1(G)=G_3$. 从而由 K 的任意性, 有 $G_3\leqslant \mathrm{Z}(G)$. 设 $G=\langle a,b\rangle$. 因为 $c(G)=3$ 和 $\mho_1(G)=G_3\leqslant Z(G)$, 所以 $[a,b,a]^p=[a,b,a^p]=1$. 同理, $[a,b,b]^p=[a,b,b^p]=1$. 又 $G_3=\langle [a,b,a],\ [a,b,b]\rangle$, 从而 $|G_3|\leqslant p^2$. 因此 $|G|\leqslant p^5$, 矛盾. 所以 $|G|=p^5$.

断言 G 非极大类, 因此 $c(G)\leqslant 3$. 若否, 根据定理 4.5.3, $p>3$. 设 $\overline{G}=G/G_4=G/\mathrm{Z}(G)$. 则 $|\overline{G}|=p^4$. 又 $p\geqslant 5$, 根据定理 4.5.4, $\exp(\overline{G})=p$. 由 p^4 阶群的分类可知, $\overline{G}$ 有一个交换的极大子群, 设为 K/G_4. 那么 K/G_4 是初等交换 p- 群. 这样, 极大子群 K 三元生成, 矛盾于 K 是 $\mathcal{A}_1$ 群.

根据定理 3.2.2, G 不是极小非亚循环群, 那么存在一个非亚循环极大子群 K, $|K|=p^4$. 设

$$K=\langle a,d \mid a^{p^2}=d^p=e^p=1,[a,d]=e,[e,a]=[e,d]=1\rangle.$$

由 $G/\Omega_1(K)$ 是 p^2 阶交换群可知, $G'\leqslant \Omega_1(K)=\langle a^p,d,e\rangle$ 和 $\exp(G')=p$.

因为 $\forall g_1,g_2\in G$, $[g_1^p,g_2]=[g_1,g_2]^{\binom{p}{1}}[g_1,g_2,g_1]^{\binom{p}{2}}=1$, 所以 $\mho_1(G)\leqslant \mathrm{Z}(G)$.

又 $\mho_1(G) \leqslant \Phi(G) < K$, 所以 $\mho_1(G) \leqslant Z(K) = \Phi(K) \leqslant \Omega_1(K)$. 因此, $\exp(G/\Phi(K)) = \exp(G/\Omega_1(K)) = p$. 这样, 由 $d(G) = 2$, $\Phi(G) = \Omega_1(K) = \langle d, \Phi(K)\rangle$.

设 $f \in G\backslash K$. 由于 $d \in \Phi(G)$, 所以 $G = \langle a, d, f\rangle = \langle a, f\rangle$.

令 $[a, f] = d^s a^{tp} e^k$. 则 $(s, p) = 1$. 若否, $G/\Phi(K)$ 是方次数为 p 的交换群, 矛盾于 $d(G) = 2$. 设 $c = d^s a^{tp} e^r$ 和 $e_1 = [a, c] = e^s$. 则 $e_1 \in G_3 \leqslant Z(G)$ 和 $c(G) = 3$. 因此 $\Phi(K) = \langle a^p, e\rangle \leqslant Z(G)$. 故 $Z(G) = \Phi(K)$.

令 $[c, f] = a^{kp} e_1^l$. 设 $b = a^l f$. 则 $[c, b] = a^{kp}$.

设 $M = \langle b, \Phi(G)\rangle = \langle b, c, Z(G)\rangle$. 因为 M 是极大子群, 所以 M 是 $\mathcal{A}_1$ 群, $(k, p) = 1$ 且 $M = \langle b, c\rangle$.

由于 $b^p \in Z(G)$, $b^{p^2} = 1$. 因为 $|M| = p^4$, 所以 $b^p \neq 1$. 设 $b^p = a^{xp} e_1^y$. 断言 $(y, p) = 1$. 若否, $[c, b] = a^{kp} = b^{x'kp}$, 其中 $xx' \equiv 1 \pmod p$, 因而 $|M| = p^3$, 矛盾. 则 $[c, a] = e_1^{-1} = a^{xy'p} b^{-y'p}$, 其中 $yy' \equiv 1 \pmod p)$. 设 $i = xy'$ 和 $j = -y'$. 则

$$G = \langle a, b \mid a^{p^2} = b^{p^2} = c^p = 1, [a, b] = c, [c, b] = a^{kp}, [c, a] = a^{ip} b^{jp}\rangle$$

其中 $(k, p) = 1$, $(j, p) = 1$.

(2) 由 (1), 有 $\Phi(G) = G' = \langle a^p, b^p, c\rangle$ 和 $Z(G) = G_3 = \langle a^p, b^p\rangle$. 因为 $c(G) = 3$ 和 $\exp(G') = p$, 所以 G 是 p- 交换群. 计算可得, $[c, ab^s] = a^{ip} b^{jp} a^{ksp} = (a^{i+ks} b^j)^p$.

设 $M = \langle \Phi(G), b\rangle$ 和 $K_s = \langle \Phi(G), ab^s\rangle$, 其中 $s = 0, 1, \ldots, p-1$. G 的极大子群分别是 M 和 K_s. M 是内交换群且 $|K_s'| = p$, 根据定理 2.1.4, G 是 $\mathcal{A}_2$ 群当且仅当对 $\forall s$, $d(K_s) = 2$, 也就是说, $|\Phi(K_s)| = p^2$. 又因为 $\Phi(K_s) = \langle (ab^s)^p, [c, ab^s]\rangle = \langle (ab^s)^p, (a^{i+ks} b^j)^p\rangle = \langle a^p b^{sp}, a^{(i+ks)p} b^{jp}\rangle$, 所以, 对 $\forall s$, $\begin{vmatrix} 1 & s \\ i+ks & j \end{vmatrix} \not\equiv 0 \pmod p$ 即对 $\forall s$, $j - (ks^2 + is) \equiv 0 \pmod p$ 无解. 由 $(k, p) = 1$ 和 $p > 2$, 从而 $i^2 + 4kj$ 是

模 p 的平方非剩余. □

定理 4.5.7. 将要给出无交换极大子群的 $\mathcal{A}_2$ 群, 且 $p \geqslant 5$.

定理 4.5.7. *设 G 是 p- 群, $p \geqslant 5$. 假设 G 非亚循环且所有的极大子群都是 $\mathcal{A}_1$ 群. 则 G 是以下互不同构的群之一:*

(1) $\langle a, b \mid a^{p^2} = b^{p^2} = c^p = 1, [a, b] = c, [c, a] = b^{\nu p}, [c, b] = a^p \rangle$, 其中 ν 是固定的模 p 的平方非剩余;

(2) $\langle a, b \mid a^{p^2} = b^{p^2} = c^p = 1, [a, b] = c, [c, a] = a^{-p} b^{-lp}, [c, b] = a^{-p} \rangle$, 其中 $4l = g^{2r+1} - 1$ 对于 $r = 1, 2, \ldots, \frac{1}{2}(p-1)$, g 是模 p 的最小原根;

证明 根据引理 4.5.6, $G = \langle a, b \mid a^{p^2} = b^{p^2} = c^p = 1, [a, b] = c, [c, b] = a^{kp}, [c, a] = a^{ip} b^{jp} \rangle$, 其中 $(k, p) = 1, (j, p) = 1$, $i^2 + 4kj$ 是模 p 的平方非剩余.

设 $a' = a^r b^s c^t, b' = a^u b^v c^w, c' = [a', b']$ 和 $x = rv - su$, 其中 r, s, t, u, v, w 是一些合适的非负整数且 $p \nmid x$, 则 $c' \equiv c^x \pmod{G_3}$. $[c', a'] = [c, a^r b^s]^x = (a^{ip} b^{jp})^{rx} a^{xskp} = a^{x(ri+sk)p} b^{xrjp}$. $[c', b'] = [c, a^u b^v]^x = a^{x(ui+vk)p} b^{xujp}$. 设 $[c', a'] = a'^{i_1 p} b'^{j_1 p}$ 和 $[c', b'] = a'^{k_1 p}$. 则有 $(j_1, p) = 1, (k_1, p) = 1$, $i_1^2 + 4k_1 j_1$ 是模 p 的平方非剩余, 且

$$\begin{cases} x(ri + sk) \equiv ri_1 + uj_1 \pmod{p} & (1) \\ xrj \equiv si_1 + vj_1 \pmod{p} & (2) \\ x(ui + vk) \equiv rk_1 \pmod{p} & (3) \\ xuj \equiv sk_1 \pmod{p} & (4) \end{cases}$$

即

$$x \begin{pmatrix} r & s \\ u & v \end{pmatrix} \begin{pmatrix} i & j \\ k & 0 \end{pmatrix} \equiv \begin{pmatrix} i_1 & j_1 \\ k_1 & 0 \end{pmatrix} \begin{pmatrix} r & s \\ u & v \end{pmatrix} \pmod{p}.$$

则 $x^2\begin{vmatrix} i & j \\ k & 0 \end{vmatrix} \equiv \begin{vmatrix} i_1 & j_1 \\ k_1 & 0 \end{vmatrix} \pmod p$. 因此 $k_1j_1 \equiv x^2kj \pmod p$.

也有 $\begin{pmatrix} i_1 & j_1 \\ k_1 & 0 \end{pmatrix} \equiv x\begin{pmatrix} r & s \\ u & v \end{pmatrix}\begin{pmatrix} i & j \\ k & 0 \end{pmatrix}\begin{pmatrix} r & s \\ u & v \end{pmatrix}^{-1} \pmod p$.

也即 $\begin{pmatrix} i_1 & j_1 \\ k_1 & 0 \end{pmatrix} \equiv x\begin{pmatrix} r & s \\ u & v \end{pmatrix}\begin{pmatrix} i & j \\ k & 0 \end{pmatrix}\begin{pmatrix} v & -s \\ -u & r \end{pmatrix}x^{-1} \pmod p$,

即 $\begin{pmatrix} i_1 & j_1 \\ k_1 & 0 \end{pmatrix} \equiv \begin{pmatrix} rvi+svk-ruj & -rsi-s^2k+r^2j \\ uvi+v^2k-u^2j & -sui-svk+ruj \end{pmatrix} \pmod p$.

则

$$\begin{cases} i_1 \equiv rvi+svk-ruj \pmod p & (5) \\ j_1 \equiv -rsi-s^2k+r^2j \pmod p & (6) \\ k_1 \equiv uvi+v^2k-u^2j \pmod p & (7) \\ 0 \equiv -sui-svk+ruj \pmod p & (8) \end{cases}$$

由 (5) 和 (8) 得到

$$i_1 \equiv ix \pmod p \qquad (5')$$

情形 I: $i=0$. 则 $i_1=0$ 和 $k_1\equiv v^2k-u^2j \pmod p$, $j_1\equiv r^2j-s^2k \pmod p$.

子情形 (i): k 是模 p 的平方剩余. 则 j 是一个固定的模 p 的平方非剩余. 在此情形, 存在整数 v_0, r_0 满足 $v_0^2k\equiv 1 \pmod p$ 和 $r_0^2j\equiv \nu \pmod p$. 其中 ν 是一个固定的模 p 的平方非剩余. 令 $r=r_0, v=v_0$ 和 $u=s=0$. 得到 $k_1=1$ 和 $j_1=\nu$. 则 G 是类型 (1).

子情形 (ii): k 是模 p 的平方非剩余. 则 j 是模 p 的平方剩余. 在此情形, 存在整数 v_0, r_0 满足 $v_0^2k\equiv\eta \pmod p$ 和 $r_0^2j\equiv 1 \pmod p$. 其中 η 是一个固定的模 p 的平方非剩余.

令 $r=r_0, v=v_0$ 和 $u=s=0$. 我们得到以下群

$$\langle a,b \mid a^{p^2}=b^{p^2}=c^p=1, [a,b]=c, [c,a]=b^p, [c,b]=a^{\eta p}\rangle$$

其中 η 是一个固定的模 p 的平方非剩余.

假设 $j=1$ 和 $k=\eta$, 其中 η 是一个最小的模 p 的平方非剩余 (也就是说, $\eta-1$ 是一个模 p 的平方剩余. 令 $r=\eta$ 和 $s=u=v=1$, 我们有 $k_1=\eta-1$ 和 $j_1=\eta^2-\eta$. 由于 $\eta-1$ 是一个模 p 的平方剩余, 所以这种情况属于情形 (i).

情形 II: $(i,p)=1$.

子情形 (i): $-k$ 是模 p 的平方剩余. 设 $v=v_0$ 满足 $-kv_0^2=1$. 令 $r=i'kv_0, v=v_0$ 和 $s=u=0$, 其中 $ii'\equiv 1 \pmod p$, 有 $x=-i', i_1=-1, k_1=-1, j_1=-i'^2kj$. 则 G 是类型 (2) 的某个群, 其中 $l\equiv i'^2kj \pmod p$.

子情形 (ii): $-k$ 是模 p 的平方非剩余且 j 是一个模 p 的平方剩余. 设 $j=e^2$ 和 $jj'\equiv 1 \pmod p$. 令 $r=u=ej', s=ei', v=0$, 我们有 $x=-i', i_1=-1, k_1=-1, j_1=-i'^2kj$. 则 G 是类型 (2) 的某个群, 其中 $l\equiv i'^2kj \pmod p$.

子情形 (iii): $-k$ 和 j 都是模 p 的平方非剩余. 设 η 是最小的模 p 的平方非剩余, 也就是说, $\eta-1$ 是模 p 的平方剩余. 在此情形, 存在整数 v_0, r_0 满足 $-v_0^2k\equiv \eta \pmod p$ 和 $r_0^2j\equiv \eta \pmod p$. 令 $r=r_0, v=v_0$ 和 $u=s=0$, 我们得到以下群:

$$\langle a,b \mid a^{p^2}=b^{p^2}=c^p=1, [a,b]=c, [c,a]=a^{ir_0v_0p}b^{\eta p}, [c,b]=a^{-\eta p}\rangle.$$

我们假设 $j=\eta$ 和 $k=-\eta$. 因为 $i^2+4kj=i^2-4\eta^2$ 是模 p 的平方剩余, 所以 $\eta(i^2-4\eta^2)$ 是一个平方. 设 $\eta(i^2-4\eta^2)=e^2$. 令 $r=i-e, s=2\eta, u=2\eta$ 和 $v=i+e$, 我们有 $x=(1-\eta)(i^2-4\eta^2)$, $i_1=(1-\eta)i(i^2-4\eta^2)$, $k_1=-\eta(i+e)^2+2i\eta(i+e)-\eta(2\eta)^2=(1-\eta)e^2$ 和 $j_1=\eta(i-e)^2-2\eta i(i-e)+\eta(2\eta)^2=(\eta-1)e^2$. 因为 $(\eta-1)e^2$ 是模 p 的平方剩余, 所以属于情形 (i).

设 G 和 H 是定理 4.5.7 中各自具有参数 i,j,k 和 i_1,j_1,k_1 的两

个群. 依照上面的证明, G 和 H 同构当且仅当存在 x 满足 $p \nmid x$, $i_1 \equiv xi \pmod p$ 和 $k_1 j_1 \equiv x^2 kj \pmod p$. 因此这两种群不同构. □

以下定理 4.5.8, 我们将要给出所有极大子群都不交换的 $\mathcal{A}_2$ 群, $p = 3$.

定理 4.5.8. 设 G 是 3- 群. 假设 G 非亚循环且所有极大子群都是 $\mathcal{A}_1$- 群. 则 G 是下列互不同构的群之一:

(1) $\langle a, b \mid a^9 = b^9 = c^3 = 1, [a, b] = c, [c, a] = b^{-3}, [c, b] = a^3 \rangle$;

(2) $\langle a, b \mid a^9 = b^9 = c^3 = 1, [a, b] = c, [c, a] = b^{-3}, [c, b] = a^{-3} \rangle$.

证明 根据引理 4.5.6, $G = \langle a, b \mid a^9 = b^9 = c^3 = 1, [a, b] = c, [c, b] = a^{3k}, [c, a] = a^{3i} b^{3j} \rangle$, 其中 $(k, 3) = 1, (j, 3) = 1$. 也有 $\Phi(G) = G' = \langle a^3, b^3, c \rangle$ 和 $\mathrm{Z}(G) = G_3 = \langle a^3, b^3 \rangle$. 我们仅需要决定满足 G 是 $\mathcal{A}_2$ 群的参数 i, j, k 的取值.

设 $K_1 = \langle \Phi(G), a \rangle$, $K_2 = \langle \Phi(G), b \rangle$, $K_3 = \langle \Phi(G), ba \rangle$ 和 $K_4 = \langle \Phi(G), ba^{-1} \rangle$. 则 G 的全部极大子群分别是 K_s (s=1,2,3,4). 我们已经知道 $K_1 = \langle c, a \rangle$, $K_2 = \langle c, b \rangle$ 都是内交换群以及 $|K_3'| = 3, |K_4'| = 3$. 那么根据定理 2.1.4, G 是 $\mathcal{A}_2$- 群当且仅当 $d(K_3) = d(K_4) = 2$, (也就是说, $|\Phi(K_3)| = |\Phi(K_4)| = 9$). 注意到 $\Phi(K_3) = \langle (ba)^3, [c, ba] \rangle$ 和 $\Phi(K_4) = \langle (ba^{-1})^3, [c, ba^{-1}] \rangle$.

情形 (i): $i = 0, j = -1, k = 1$. G 是类型 (1).

通过计算, $(ba)^3 = b^3 a^3 [b, a^{-1}, a^{-1}][b, a^{-1}, b] = b^6 a^6$, $[c, ba] = a^3 b^{-3}$, $(ba^{-1})^3 = b^3 a^{-3} [b, a, a][b, a, b] = b^6 a^3$ 和 $[c, ba^{-1}] = a^3 b^3$. 因为 $|\Phi(K_3)| = |\Phi(K_4)| = 9$, 所以 G 是 $\mathcal{A}_2$ 群.

情形 (ii): $i = 0, j = -1, k = -1$. G 是类型 (2).

通过计算, $(ba)^3 = b^3 a^3 [b, a^{-1}, a^{-1}][b, a^{-1}, b] = b^{-3}$, $[c, ba] = a^{-3} b^{-3}$, $(ba^{-1})^3 = b^3 a^{-3} [b, a, a][b, a, b] = b^{-3}$ 和 $[c, ba^{-1}] = a^{-3} b^3$. 因为 $|\Phi(K_3)| = |\Phi(K_4)| = 9$, 所以 G 是 $\mathcal{A}_2$ 群.

情形 (iii): $i=0, j=1, k=1$. $G=\langle a,b \mid a^9=b^9=c^3=1, [a,b]=c, [c,a]=b^3, [c,b]=a^3\rangle$. 设 $a'=b, b'=a$ 和 $c'=[a',b']$. 则 $a'^3=b^3, b'^3=a^3, [a',b',a']=[b,a,b]=a^{-3}=b'^{-3}$, $[a',b',b']=[b,a,a]=b^{-3}=a'^{-3}$. 因而 a', b' 满足类型 (2) 的定义关系.

情形 (iv): $i=0, j=1, k=-1$. $G=\langle a,b \mid a^9=b^9=c^3=1, [a,b]=c, [c,a]=b^3, [c,b]=a^{-3}\rangle$. 因为 $[c,ba]=[c,b][c,a]=a^{-3}b^3$ 和 $(ba)^3=b^3a^3[b,a^{-1},b][b,a^{-1},a^{-1}]=b^3a^3[a,b,b][a,b,a]^{-1}=1$, 所以 $|\Phi(K_3)|=3$. 因此 G 不是 $\mathcal{A}_2$ 群.

情形 (v): $i=1, j=1, k=1$. $G=\langle a,b \mid a^9=b^9=c^3=1, [a,b]=c, [c,a]=a^3b^3, [c,b]=a^3\rangle$. 因为 $[c,ba^{-1}]=[c,b][c,a]^{-1}=b^{-3}$ 和 $(ba^{-1})^3=b^3a^{-3}[b,a,b][b,a,a]=1$, 所以 $|\Phi(K_4)|=3$. 因此 G 不是 $\mathcal{A}_2$ 群.

情形 (vi): $i=1, j=1, k=-1$. $G=\langle a,b \mid a^9=b^9=c^3=1, [a,b]=c, [c,a]=a^3b^3, [c,b]=a^{-3}\rangle$. 设 $a'=b^{-1}, b'=a^{-1}b^{-1}, c'=[a',b']$. 则 $a'^3=b^{-3}$,

$$
\begin{aligned}
b'^3 &= (a^{-1}b^{-1})^3=a^{-3}b^{-3}[a^{-1},b]^{\binom{3}{2}}[a^{-1},b,b][a^{-1},b,a^{-1}] \\
&= a^{-3}b^{-3}a^3a^3b^3=a^3
\end{aligned}
$$

$[a',b',a']=[b^{-1},a^{-1}b^{-1},b^{-1}]=[b^{-1},a^{-1},b^{-1}]=[a,b,b]=a^{-3}=b'^{-3}$, $[a',b',b']=[b^{-1},a^{-1}b^{-1},a^{-1}b^{-1}]=[b^{-1},a^{-1},a^{-1}]\,[b^{-1},a^{-1},b^{-1}]=[a,b,a][a,b,b]=b^3=a'^{-3}$. 这样, a', b' 满足类型 (2) 的定义关系.

情形 (vii): $i=1, j=-1, k=1$. $G=\langle a,b \mid a^9=b^9=c^3=1, [a,b]=c, [c,a]=a^3b^{-3}, [c,b]=a^3\rangle$. 因为 $[c,ba^{-1}]=[c,b][c,a]^{-1}=b^3$ 和 $(ba^{-1})^3=b^3a^{-3}[b,a,b][b,a,a]=b^{-3}$, 所以 $|\Phi(K_4)|=3$. 因此 G 不是 $\mathcal{A}_2$ 群.

情形 (viii): $i=1, j=-1, k=-1$. $G=\langle a,b \mid a^9=b^9=c^3=1, [a,b]=c, [c,a]=a^3b^{-3}, [c,b]=a^{-3}\rangle$. 因为 $[c,ba^{-1}]=[c,b][c,a]^{-1}=a^3b^3$ 和 $(ba^{-1})^3=b^3a^{-3}[b,a,b][b,a,a]=a^{-3}b^{-3}$, 所以 $|\Phi(K_4)|=3$. 因

此 G 不是 $\mathcal{A}_2$ 群.

情形 (ix): $i=-1$. 设 $b'=b^{-1}, c'=[a,b']$. 则 $[c',a]=[a,b',a]=[a,b^{-1},a]=[a,b,a]^{-1}=a^3b'^{3j}$, $[c',b']=[a,b',b']=[a,b^{-1},b^{-1}]=[a,b,b]=a^{3k}$. 属于情形 (v)-(viii).

下面证明类型 (1) 和类型 (2) 互不同构.

设 $V_1(G)=\{g^3 \mid g\in G\}$. 则 $V_1(G)=\{(a^mb^nc^l)^3 \mid m,n\leqslant 9, l\leqslant 3\}$. 经计算,

$$\begin{aligned}(a^mb^nc^l)^3 &= (a^mb^n)^3c^{3l}[a^mb^n,c^{-l},c^{-l}][a^mb^n,c^{-l},a^mb^n]\\ &= (a^mb^n)^3\\ &= a^{3m}b^{3n}[a^m,b^{-n},b^{-n}][a^m,b^{-n},a^m]\\ &= a^{3m(1+kn^2-mni)}b^{3n(1-m^2j)}\end{aligned}$$

对于类型 (1),

$$(a^mb^nc^l)^3=\begin{cases} b^{3n} & m\equiv 0 \pmod 3\\ a^{3(1+n^2)}b^{6n}=\begin{cases} a^3 & n\equiv 0 \pmod 3\\ a^{-3}b^{-3} & n\equiv 1 \pmod 3\\ a^{-3}b^3 & n\equiv 2 \pmod 3\end{cases} & m\equiv 1 \pmod 3\\ a^{6(1+n^2)}b^{6n}=\begin{cases} a^{-3} & n\equiv 0 \pmod 3\\ a^3b^{-3} & n\equiv 1 \pmod 3\\ a^3b^3 & n\equiv 2 \pmod 3\end{cases} & m\equiv 2 \pmod 3\end{cases}$$

对于类型 (2),

$$(a^nb^mc^l)^3 = \begin{cases} b^{3n} & m \equiv 0 \pmod 3 \\ a^{3(1-n^2)}b^{-3n} = \begin{cases} a^3 & n \equiv 0 \pmod 3 \\ b^{-3} & n \equiv 1 \pmod 3 \\ b^3 & n \equiv 2 \pmod 3 \end{cases} & m \equiv 1 \pmod 3 \\ a^{6(1-n^2)}b^{-3n} = \begin{cases} a^{-3} & n \equiv 0 \pmod 3 \\ b^{-3} & n \equiv 1 \pmod 3 \\ b^3 & n \equiv 2 \pmod 3 \end{cases} & m \equiv 2 \pmod 3 \end{cases}$$

对于类型 (1), $|V_1(G)| = 9$, 对于类型 (2), $|V_1(G)| = 5$. 因此这两种群不同构. □

§4.6 小结

本节我们给出 $\mathcal{A}_2$ 群的群表并得出一些有用的推论.

定理 4.6.1. 设 G 是有限 p 群. 则 G 是 $\mathcal{A}_2$ 群当且仅当 G 同构于下列群之一:

一. 亚循环 $\mathcal{A}_2$ 群:

(1) $< r, s, t, u >_p$ 满足 $s + u = 2$, 并且若 $p = 2$, 则 $r \geqslant 2$.

(2) 16 阶二面体群, 半二面体群和广义四元数群.

(3) $< r, s, v, t, t', u >_2$ 其中 $r = 3$, $s = v = t' = u = 0$, $t \geqslant 0$.

(4) $< r, s, v, t, t', u >_2$ 其中 $r = 2$, $s + v + t' + u = 1$, $t \geqslant 0$.

二. 非亚循环 $\mathcal{A}_2$ 群且 $|G| = p^4$:

(1) 若 $p = 2$, G 是 $D_8 \times C_2$, 或 $Q_8 \times C_2$, 或中心积 $D_8 * C_4$.

(2) 若 $p > 2$, G 是 $M \times C_p$, 其中 M 为 p^3 阶非交换群 (M 有两种互不同构的形式), 或以下互不同构的群之一:

(i) $\langle a, b, c \mid a^{p^2} = b^p = c^p = 1, [b, c] = a^p, [a, b] = [a, c] = 1\rangle$;

(ii) $\langle a, b, c, d \mid a^p = b^p = c^p = d^p = 1, [c, d] = b, [b, d] = a, [a, b] = [a, c] = [a, d] = [b, c] = 1\rangle$;

(iii) $\langle a,b,c \mid a^{p^2}=b^p=1, c^p=a^{\alpha p}, [a,b]=a^p, [a,c]=b, [b,c]=1\rangle$. 其中 $\alpha=0,1$ 或是一个模 p 的平方非剩余 (三种互不同构的群);

(iv) $p=3$, $\langle a,b,c \mid a^9=b^3=c^3=1, [a,b]=1, [a,c]=b, [c,b^{-1}]=a^{-3}\rangle$.

三. 有交换极大子群的 $\mathcal{A}_2$ 群且 $d(G)=2$: (此时, p 为奇数)

(1) $\langle b,a_1,a_2,a_3 \mid b^{p^{n-3}}=a_1^p=a_2^p=a_3^p=1, [a_1,b]=a_2, [a_2,b]=a_3, [a_i,a_j]=1, [a_3,b]=1\rangle$, 其中 $1\leqslant i,j\leqslant 3$;

(2) $\langle b,a_1,a_2 \mid b^{p^{n-2}}=a_1^p=a_2^p=1, [a_1,b]=a_2, [a_2,b]=b^{p^{n-3}}, [a_1,a_2]=1, [b^{p^{n-3}},a_1]=[b^{p^{n-3}},a_2]=1\rangle$;

(3) $\langle b,a_1,a_2 \mid b^{p^{n-3}}=a_1^{p^2}=a_2^p=1, [a_1,b]=a_2, [a_2,b]=a_1^{\nu p}, [a_1,a_2]=1, [a_1^p,b]=[a_1^p,a_2]=1\rangle$, 其中 $\nu=1$ 或者 ν 是一个固定的模 p 的平方非剩余.

四. 有交换极大子群的 $\mathcal{A}_2$ 群且 $d(G)=3$

(1) $\langle a,b\rangle\times C_p$, 其中 $\langle a,b\rangle$ 是亚循环极小非交换 p- 群且 $|\langle a,b\rangle|\geqslant p^4$; $(|G|=p^{m+n+1})$

(2) $\langle a,b\rangle\times C_p$, 其中 $\langle a,b\rangle$ 是非亚循环极小非交换 p- 群且 $|\langle a,b\rangle|\geqslant p^4$, 即 $G=\langle a,b,d \mid a^{p^m}=b^{p^n}=c^p=d^p=1, [a,b]=c, [c,a]=[c,b]=[d,a]=[d,b]=1\rangle$ 其中 $m\geqslant n$, $n\geqslant 2$; $(|G|=p^{m+n+2})$

(3) $\langle a,b\rangle * C_{p^2}$, 其中 $\langle a,b\rangle$ 是非亚循环非交换 p- 群且 $|\langle a,b\rangle|\geqslant p^4$, 即 $G=\langle a,b,d \mid a^{p^m}=b^{p^n}=d^{p^2}=1, [a,b]=d^p, [d,a]=[d,b]=1\rangle$, 其中 $m\geqslant n$, $n\geqslant 2$; $(|G|=p^{m+n+2})$

(4) $p=2$. $G=\langle a,b,c \mid a^4=b^4=1, c^2=a^2b^2, [a,b]=b^2, [c,a]=a^2, [c,b]=1\rangle$; $(|G|=2^5)$

(5) $\langle a,b\rangle\rtimes C_p$, 其中 $\langle a,b\rangle$ 是亚循环极小非交换 p 群, 即 $G=\langle a,b,d \mid a^{p^m}=b^{p^2}=d^p=1, [a,b]=a^{p^{m-1}}, [d,a]=b^p, [d,b]=1\rangle$, 若 $p=2$, $m\geqslant 3$; $(|G|=p^{m+3})$

(6) $\langle a,b,d \mid a^{p^m}=b^{p^2}=d^{p^2}=1, [a,b]=d^p, [d,a]=b^{jp}, [d,b]=1\rangle$, $(j,p)=1$, $p>2$, j 是一个固定的模 p 的平方非剩余且满足 $-4j$ 是模 p 的平方非剩余; $(|G|=p^{m+4})$

(7) $\langle a,b,d \mid a^{p^m}=b^{p^2}=d^{p^2}=1,[a,b]=d^p,[d,a]=b^{jp}d^p,[d,b]=1\rangle$, $(j,p)=1$ 且满足 $1-4j$ 是模 p 的平方非剩余. 满足这个定义关系的群有 $\frac{p-1}{2}$ 个, 若 $p=2$, $j=1$. ($|G|=p^{m+4}$)

五. 无交换极大子群的 $\mathcal{A}_2$- 群

(i) $p=2$

$G=\langle a,b,d \mid a^4=b^4=d^4=1,\ [a,b]=d^2,\ [d,a]=b^2d^2,\ [d,b]=a^2b^2\rangle$.

(ii) $p>2$

(1) $\langle a,b \mid a^{p^2}=b^{p^2}=c^p=1,[a,b]=c,[c,a]=b^{\nu p},[c,b]=a^p\rangle$, 其中 ν 是固定的模 p 的平方非剩余;

(2) $\langle a,b \mid a^{p^2}=b^{p^2}=c^p=1,[a,b]=c,[c,a]=a^{-p}b^{-lp},[c,b]=a^{-p}\rangle$, 其中 $4l=g^{2r+1}-1$ 对于 $r=1,2,\ldots,\frac{1}{2}(p-1)$, g 是模 p 的最小原根;

(3) $\langle a,b \mid a^9=b^9=c^3=1,[a,b]=c,[c,a]=b^{-3},[c,b]=a^3\rangle$;

(4) $\langle a,b \mid a^9=b^9=c^3=1,[a,b]=c,[c,a]=b^{-3},[c,b]=a^{-3}\rangle$.

为了应用方便, 我们给出下面的两个推论:

推论 4.6.2. 设 G 为导群初等交换的 $\mathcal{A}_2$ 群, 且 $c(G)>2$, 则 G 为以下互不同构的群之一:

(1) p^4 阶的极大类 p 群 (p 为奇数):

(i) $\langle a,b,c,d \mid a^p=b^p=c^p=d^p=1,[c,d]=b,[b,d]=a,[a,b]=[a,c]=[a,d]=[b,c]=1\rangle$;

(ii) $\langle a,b,c \mid a^{p^2}=b^p=1,c^p=a^{\alpha p},[a,b]=a^p,[a,c]=b,[b,c]=1\rangle$, 其中 $\alpha=0,1$ 或是一个模 p 的平方非剩余 (三种互不同构的群);

(iii) $p=3$, $\langle a,b,c \mid a^9=b^3=c^3=1,[a,b]=1,[a,c]=b,[c,b^{-1}]=a^{-3}\rangle$.

(2) 二元生成有交换极大子群的 $\mathcal{A}_2$ 群 ($n\geq 5$, p 为奇数):

(i) $\langle b,a_1,a_2,a_3 \mid b^{p^{n-3}}=a_1^p=a_2^p=a_3^p=1,[a_1,b]=a_2,[a_2,b]=a_3,\ [a_i,a_j]=1,[a_3,b]=1\rangle$, 其中 $1\leqslant i,j\leqslant 3$;

(ii) $\langle b, a_1, a_2 \mid b^{p^{n-2}} = a_1^p = a_2^p = 1, [a_1, b] = a_2, [a_2, b] = b^{p^{n-3}}, [a_1, a_2] = 1, [b^{p^{n-3}}, a_1] = [b^{p^{n-3}}, a_2] = 1\rangle$;

(iii) $\langle b, a_1, a_2 \mid b^{p^{n-3}} = a_1^{p^2} = a_2^p = 1, [a_1, b] = a_2, [a_2, b] = a_1^{\nu p}, [a_1, a_2] = 1, [a_1^p, b] = [a_1^p, a_2] = 1\rangle$, 其中 $\nu = 1$ 或者 ν 是一个固定的模 p 的平方非剩余.

(3) 无交换极大子群的 $\mathcal{A}_2$ 群 $(p \geqslant 5)$:

(i) $\langle a, b \mid a^{p^2} = b^{p^2} = c^p = 1, [a, b] = c, [c, a] = b^{\nu p}, [c, b] = a^p\rangle$, 其中 ν 是固定的模 p 的平方非剩余;

(ii) $\langle a, b \mid a^{p^2} = b^{p^2} = c^p = 1, [a, b] = c, [c, a] = a^{-p}b^{-lp}, [c, b] = a^{-p}\rangle$, 其中 $4l = g^{2r+1} - 1$ 对于 $r = 1, 2, \ldots, \frac{1}{2}(p-1)$, g 是模 p 的最小原根;

(4) 无交换极大子群的 $\mathcal{A}_2$ 群 $(p = 3)$:

(i) $\langle a, b \mid a^9 = b^9 = c^3 = 1, [a, b] = c, [c, a] = b^{-3}, [c, b] = a^3\rangle$;

(ii) $\langle a, b \mid a^9 = b^9 = c^3 = 1, [a, b] = c, [c, a] = b^{-3}, [c, b] = a^{-3}\rangle$.

推论 4.6.3. 设 G 为导群初等交换的 $\mathcal{A}_2$ 群, 且 $c(G) > 2$, 则 $d(G) = 2$ 且 p 为奇素数.

第五章 $\mathcal{T}_4$ 群

我们称有限 p 群 G 为 $\mathcal{T}_4$ 群, 如果 G 的任意两个不交换的元素都生成 p^4 阶的内交换群. 文献 [12] 完全分类了 $\mathcal{T}_4$ 群. 本书第七章将用 $\mathcal{T}_4$ 群的分类. 到本章的结果主要取自文献 [12].

§5.1 $\mathcal{T}_4$ 群的分类

我们首先给出非交换的 $\mathcal{T}_4$ 群七条性质.

定理 5.1.1. *若 G 为 $\mathcal{T}_4$ 群, 则 G 有以下性质:*

(1) $\exp G \leqslant p^3$;

(2) $\mho_1(G) \leqslant Z(G)$;

(3) $c(G) = 2$;

(4) $\Omega_1(G)$ 为交换群;

(5) G' 为初等交换 p 群;

(6) 对任意的 $a \in G$, 都有 $C_G\langle a\rangle \trianglelefteq G$;

(7) $G \times C_p{}^n$ 也为 $\mathcal{T}_4$ 群.

证明: (1) 若 G 为 $\mathcal{T}_4$ 群, 则 $\exp G \leqslant p^3$. 若否, 则存在 $g \in G$, 使得 $o(g) \geqslant p^4$, 则 $g \in Z(G)$ (若否, 则存在 $x \in G$, 使得 $\langle g, x\rangle$ 为 p^4 阶内交换群, 矛盾). 又由 G 非交换知, 存在 $c, d \in G$, 使得 $\langle c, d\rangle$ 为 p^4 阶内交换群. 考虑 cg 的阶, 同理可得 $cg \in Z(G)$, 进而 $c \in Z(G)$ 矛盾, 故 $\exp G \leqslant p^3$.

(2) 对任意的 $a, b \in G$, 若 $[a, b] = 1$, 则 $[a^p, b] = 1$; 若 $[a, b] \neq 1$, 则 $H = \langle a, b\rangle$ 为 p^4 阶的内交换群. 而 $\langle a^p, b\rangle < H$, 从而 $[a^p, b] = 1$, 由 a, b 的任意性有 $\mho_1(G) \leqslant Z(G)$.

(3) 首先证明 G 满足 2 次 *Engel* 条件. 对任意的 $a, b \in G$, 若 $[a, b] = 1$, 显然有 $[a, b, b] = 1$. 若 $[a, b] \neq 1$, 则 $H = \langle a, b\rangle$ 为 p^4 阶内交换群. 从而 $[a, b] \leqslant Z(H)$, 显然也有 $[a, b, b] = 1$. 从而 G 满足 2 次 *Engel* 条件且 $c(G) \leqslant 3$, 特别的当 G 中无 3 阶元素时 $c(G) \leqslant 2$.

再来证明 $c(G) = 2$. 若否, 则 $p = 3$, 且 $c(G) = 3$, 此时存在 $x, y, z \in G$, 使得 $[x, y, z] \neq 1$, 令 $H = \langle x, y\rangle$, 则可推出 $[x, y] \notin Z(G)$, 又由 $\mho_1(G) \leqslant Z(G)$, 可

知 $[x,y]\notin \mho_1(H)$, 从而 $\langle x,y\rangle\cong N_{2,1,3}$. 此时由

$$[x,yz,yz]=1=[x,y,y][x,y,z][x,z,y][x,z,z]$$

及 G 满足 2 次 *Engel* 条件易知 $[x,y,y]=[x,z,z]=1$, 可得 $[x,y,z][x,z,y]=1$, 由 $[x,y,z]\neq 1$ 可知 $[x,z,y]\neq 1$, 同理 $\langle x,z\rangle\cong N_{2,1,3}$. 此时 $o([x,z])=p$, $o(y)=p$, 因为 p^4 阶内交换群均不能由 p 阶元和 p 阶元生成, 从而 $[x,z,y]=1$, 进而得出 $[x,y,z]=1$, 矛盾.

(4) 因为 p^4 阶内交换群只能是 $M_{3,1,p}$、$M_{2,2,p}$、$N_{2,1,p}$, 而它们均不能由 p 阶元和 p 阶元生成, 从而任意两个 p 阶元均交换, 即 $\Omega_1(G)$ 为交换群.

(5) 对任意的 $x\in C_G\langle a\rangle$, $y\in G$, 若 $[x,y]\neq 1$, 则 $\langle x,y\rangle$ 为 p^4 阶内交换群, 从而 $o([x,y])=p$. 又由 (3) 可知 $G'\leqslant Z(G)$ 是交换群, 故 $G'=\langle [x,y]\mid x,y\rangle$ 一定是初等交换 p 群.

(6) 对任意的 $x\in C_G\langle a\rangle$, $y\in G$. 由 (3) $[x,y]\in G'\leqslant Z(G)\leqslant C_G\langle a\rangle$, 从而 $x^y=x[x,y]\in C_G\langle a\rangle$.

故 $C_G\langle a\rangle\trianglelefteq G$.

(7) 只需考虑 $G\times C_p$ 即可. 对任意的 $a,b\in G\times C_p$, 可设 $x=ac_1$, $y=bc_2$ 其中 $a,b\in G$, c_1、$c_2\in C_2$, 则 $o(x)=o(ac_1)=o(a)$, $o(y)=o(bc_2)=o(b)$. 考虑 $H=\langle x,y\rangle$ 和 $M=\langle a,b\rangle$, 若 $M=\langle a,b\rangle$ 交换, 则 $H=\langle x,y\rangle$ 也交换, 若 $M=\langle a,b\rangle$ 非交换, 由 T_4 群定义可知 M 为 p^4 内交换群, 又有 $\Phi(H)=\Phi(M)$, 故 $H=\langle x,y\rangle$ 也为 p^4 内交换群. □

引理 5.1.2. 设 G 为非交换 T_4 群, 若 G 有子群同构于 $M_{3,1,p}$, 则 G 有下列性质:

(1) $\exp G=p^3$;

(2) 对任意的 $a\in G$, 且 $o(a)=p^3$, 都有 $\langle a\rangle\trianglelefteq G$.

证明: (1) 若否, 则 $\exp G<p^3$, 或 $\exp G\geqslant p^4$, 若 $\exp G<p^3$, 与 G 有子群同构于 $M_{3,1,p}$ 矛盾. 若 $\exp G\geqslant p^4$, 则存在 $a\in G$, 使得 $o(a)\geqslant p^4$, 此时 $a\in Z(G)$(若否, 存在 $b\in G$, 使得 $[a,b]\neq 1$, 由题设存在 $a,b\in G$, 为 p^4 阶内交换群, 与 p^4 阶内交换群方次数小于等于 p^3 矛盾). 又因为 G 有子群同构于 $M_{3,1,p}$, 所以存在 $c,d\in G$, 使得 $\langle c,d\mid c^{p^3}=d^p=1,[c,d]=c^{p^2}\rangle$. 同理 $ac\in Z(G)$, 从而可知 $c\in Z(G)$, 与 $[c,d]\neq 1$ 矛盾.

(2) 对任意的 $b \in G$, 若 $[a,b]=1$, 显然 b 正规化 $\langle a\rangle$; 若 $[a,b]\neq 1$, 由题设 $\langle a,b\rangle \cong M_{3,1,p}$, 又 $o(a)=p^3$, 从而有 $\langle a\rangle \lessdot \langle a,b\rangle$, 即 $\langle a\rangle \trianglelefteq \langle a,b\rangle$, 从而 b 正规化 $\langle a\rangle$, 由 b 的任意性可知 $\langle a\rangle \trianglelefteq G$. □

定理 5.1.3. 设 G 为非交换 T_4 群, 若 G 有子群同构于 $M_{3,1,p}$, 则: $G\cong M_{3,1,p}\times C_p^n$, 其中 n 为非负整数.

证明: 由题设可知, 存在 $a,b\in G$, 使得 $H=\langle a,b \mid a^{p^3}=b^p=1,[a,b]=a^{p^2}\rangle \cong M_{3,1,p}$, 对任意的 $x\in G$, 考虑 $\langle a,x\rangle$, $\langle ab,x\rangle$. 由引理 5.1.2(2) 可知, $[x,a]\in\langle a^{p^2}\rangle = H'$, $[x,ab]\leqslant \langle (ab)^{p^2}\rangle = \langle a^{p^2}\rangle = H'$, 又由 $c(G)=2$ 以及 $H=\langle a,ab\rangle$, 所以 $[x,H]\leqslant H'$. 由 x 的任意性可得 $[G,H]\leqslant H'$, 从而 $G=H*C_G(H)$.

以下断言 (1): $\exp C_G(H)\leqslant p^2$.

若否, 存在 $c\in C_G(H)$, 且 $o(c)=p^3$, 考虑 $[a,cb]=a^{p^2}\neq 1$, 由 G 为 T_4 群, 必有 $K=\langle a,cb\rangle\cong M_{3,1,p}$, 从而 $\langle a^p\rangle=\langle c^p\rangle=\Phi(K)$, 即存在 l 使得 $(l,p)=1$ 且 $a^p=c^{lp}$, 此时 $o(ac^{-l})=p$, 再考虑 $\langle ac^{-l},b\rangle$, 与定理 5.1.1(4) 矛盾.

以下断言 (2): $C_G(H)$ 为交换群.

若否, 存在 $K\leqslant C_G(H)$, 由 G 为 T_4 群和 $\exp C_G(H)\leqslant p^2$ 可知 $K\cong M_{2,2,p}$ 或 $N_{2,1,p}$.

若 $K\cong M_{2,2,p}$, 不妨设 $K=\langle c,d \mid c^{p^2}=d^{p^2}=1,[c,d]=c^p\rangle$. 考虑 $\langle ac,d\rangle$, $[ac,d]=[c,d]=c^p\neq 1$, 由 G 为 T_4 群可知 $\langle ac,d\rangle\cong M_{3,1,p}$, 且存在 k,l, 使得 $c^p=(ac)^{kp^2}=d^{lp}((k,p)=1,\ (l,p)=1)$, 与 $K\cong M_{2,2,p}$ 矛盾.

若 $K\cong N_{2,1,p}$, 不妨设 $K=\langle c,d \mid c^{p^2}=d^p=e^p=1,[c,d]=e,[e,c]=[e,d]=1\rangle$. 考虑 $\langle ad,c\rangle$, 由定理 5.1.1(3) 可知 $[ad,c]=[c,d]=e^{-1}\neq 1$, 由 G 为 T_4 群可知 $\langle ad,c\rangle\cong M_{3,1,p}$, 从而存在 k,l 有 $e^{-1}=(ad)^{kp^2}=c^{lp}((k,p)=1,\ (l,p)=1)$, 与 $K\cong N_{2,1,p}$ 矛盾. 故 $C_G(H)$ 为交换群.

由 $\exp C_G(H)\leqslant p^2$, 可令 $C_G(H)=C_{p^2}^{k_1}\times C_p^{k_2}$, (其中 k_1, k_2 为非负整数.) 则 $G=H*C_G(H)=H*(C_{p^2}^{k_1}\times C_p^{k_2})=H\times C_{p^2}^{l_1}\times C_p^{l_2}$. 容易证明 $l_1=0$. 否则, 必然存在直积因子 $\langle b_1\rangle\in C_G(H)$ 其中 $o(b_1)=p^2$, 考虑 $\langle a,b_1b\rangle$, $[a,b_1b]=[a,b]=a^{p^2}\neq 1$, 由 G 为 T_4 群可知 $\langle a,b_1b\rangle\cong M_{3,1,p}$. 从而存在 l 使得 $a^{p^2}=(b_1b)^{lp}=b_1^{lp}$((l,p)=1), 矛盾于 $\langle a\rangle\cap\langle b_1\rangle=1$, 故 $G=M_{3,1,p}\times C_p^n$.

再来证明 $M_{3,1,p}\times C_p^n$ 为 T_4 群. 由定理 5.1.1(7) 立得. □

引理 5.1.4. 设 G 为非交换的 T_4 群. 且 G 所有的二元生成的非交换子群全为 $M_{2,2,2}$, 则 G 有以下性质:

(1) $\exp G=2^2$;

(2) 对任意的 $a,b\in G$, 若 $[a,b]\neq 1$ 且 $a^2\neq b^2$, 则 $[a,b]=a^2$ 或 b^2;

(3) $\Omega_1(G)=Z(G)$.

证明: (1)(反证法) 若否, 则存在 $g\in G$ 使得 $o(g)=2^3$, 由题设 $g\in Z(G)$. (若否存在 $c\in G$ 使得 $[c,g]\neq 1$, 从而 $\langle c,g\rangle\cong M_{2,2,2}$, 矛盾.) 又由 G 非交换知必存在 $a,b\in G$ 使得 $\langle a,b\mid a^4=b^4=1,[a,b]=a^2\rangle\cong M_{2,2,2}$, 同理 $ag\in Z(G)$, 从而 $a\in Z(G)$, 与 $[a,b]\neq 1$ 矛盾.

(2) 若 $[a,b]\neq 1$, 由题设有 $\langle a,b\rangle\cong M_{2,2,2}$. 从而 $\Omega_1(\langle a,b\rangle)=\Phi(\langle a,b\rangle)=\mho_1(\langle a,b\rangle)=Z(\langle a,b\rangle)\cong C_2\times C_2$, 从而 $o(a)=o(b)=4$. 且 $\langle a^2,b^2\rangle\leqslant\Phi(\langle a,b\rangle)=\mho_1(\langle a,b\rangle)\cong C_2\times C_2$. 又若 $a^2\neq b^2$, 则 $\langle a^2,b^2\rangle=\Phi(\langle a,b\rangle)\cong C_2\times C_2$. 从而 $[a,b]\in\langle a^2,\ b^2\rangle$, 又因为 $[a,b]\neq 1,a^2,b^2$, 所以 $[a,b]=a^2b^2$, 此时 $(ab)^2=a^2b^2[a,b]=1$, 从而 $ab\in\Omega_1(\langle a,b\rangle)=Z(\langle a,b\rangle)$ 与 $[a,b]\neq 1$ 矛盾.

(3) 先证 $\Omega_1(G)\leqslant Z(G)$. 只需证 $\Lambda_1(G)\subseteq Z(G)$ 即可. (反证法) 若否, 则存在 $a\in\Lambda_1(G)$, 且 $a\notin Z(G)$, 从而存在 $b\in G$, 使得 $[a,b]\neq 1$, 由题设 $\langle a,b\rangle\cong M_{2,2,2}$, 则 $a\in\Omega_1(\langle a,b\rangle)=Z(\langle a,b\rangle)$ 与 $[a,b]\neq 1$ 矛盾, 从而 $\Omega_1(G)\leqslant Z(G)$. 再证 $\Omega_1(G)\geqslant Z(G)$, 只需证 $\exp Z(G)=2$, 若否, 存在 $g\in Z(G)$, 且 $o(g)=4$ 又因为 G 非交换, 不妨设存在 a,b, 使得 $[a,b]\neq 1$, 由题设不妨设 $\langle a,b\mid a^4=b^4=1,[a,b]=a^2\rangle\cong M_{2,2,2}$, 考虑 $[ag,b]=a^2\neq 1,(ag)^2,b^2$, 由引理 5.1.4(2) 有 $(ag)^2=b^2$, 再考虑 $[a,gb]=a^2=(gb)^2$, 从而 $\langle a,gb\rangle\cong Q_8$, 与题设矛盾. 从而有 $\Omega_1(G)\geqslant Z(G)$, 从而有 $\Omega_1(G)=Z(G)$. □

定理 5.1.5. 设 G 为非交换的 T_4 群. 若 G 的所有的二元生成的非交换子群均同构于 $M_{2,2,2}$, 则 G 为下列互不同构的群之一:

(1) $H\times C_2^n$, 其中 $H=K\rtimes\langle b\rangle$ 是 $K=\langle a_1\rangle\times\langle a_2\rangle\times\cdots\times\langle a_l\rangle\cong C_4^l$ 被 $\langle b\rangle$ 的循环扩张, 满足 $a_i^b=a_i^{-1}$ 对任意的 $1\leqslant i\leqslant l$ 成立. 其中 n 为非负整数, l 为正整数;

(2) $H \times C_2^n$. 其中 $H = \langle a_1, a_2, b \mid a_1^4 = a_2^4 = 1, b^2 = a_1^2, [a_1, b] = a_2^2, [a_2, b] = a_1^2, [a_1, a_2] = 1\rangle$, n 为非负整数;

(3) $H \times C_2^n$. 其中 $H = \langle a_1, a_2, b, d \mid a_1^4 = a_2^4 = 1,\ b^2 = a_1^2, d^2 = a_2^2, [a_1, a_2] = 1, [a_1, b] = a_2^2,\ [a_2, b] = a_1^2,\ [a_1, d] = a_1^2,\ [a_2, d] = a_1^2a_2^2, [b, d] = 1\rangle$, n 为非负整数.

证明: 令 H 为 G 的最大阶的交换子群, 由引理 5.1.4(1) 可设 $H = A \times C$, 其中 $A = \langle a_1\rangle \times \langle a_2\rangle \times \cdots \times \langle a_l\rangle \cong C_4^l$, $C = \langle b_1\rangle \times \langle b_2\rangle \times \cdots \times \langle b_k\rangle \cong C_2^k$.

从而有 $H \trianglelefteq G$(对任意的 $h \in H, g \in G$, 由定理 5.1.1 可知, $[h, g] \in Z(G) \leqslant H$.), 且对任意 G 中的 4 阶元 g, 均有 $g^2 \in H$.

由 H 的最大性和引理 5.1.4 可知, $Z(G) = \Omega_1(G) = \Omega_1(H) = \Omega_1(A) \times C$. 再由定理 5.1.1 可知 $G' \leqslant \Omega_1(H)$ 且 $G/\Omega_1(H)$ 是初等交换 2 群.

以下有断言 1: 对任意的 $a_i \in H$, $g \in G \setminus H$, 有 $[a_i, g] \neq 1$. (反证法) 若否, 不妨设 $[a_1, g] = 1$, 由 H 的最大性, 则存在 $h \in H$, 使得 $[h, g] \neq 1$. 考虑 $\langle h, a_1, g\rangle$, 显然 $a_1 \in Z(\langle h, a_1, g\rangle)$. 由题设性质子群遗传, 与引理 5.1.4(3) 矛盾. 所以断言成立. 以下分两种情况讨论:

情况一.对所有的 $b \in G \setminus H$, 均有 $b^2 \notin \mho_1(H)$.

此时断言 2: $[a_i, b] \neq b^2$. 若否 $(a_ib)^2 = a_i^2$, 即存在 $a_ib \in G \setminus H$, 且 $(a_ib)^2 \in \mho_1(H)$, 矛盾. 又由断言 1, $[a_i, b] \neq 1$. 又由 $b^2 \notin \mho_1(H)$. 从而 $a_i^2 \neq b^2$, 再由引理 5.1.4(2) 即可得 $[a_i, b] = a_i^2$. 同理对任意的 $d \in G \setminus H$ 我们也有 $[a_i, d] = a_i^2$. 从而 $[a_i, bd] = 1$, $bd \in C_G(H)$. 再由 H 的取法可知 $bd \in H$, 进而 $d \in \langle H, b\rangle$, 这就说明 $G = \langle H, b\rangle$ 同构于定理中出 (1) 型群.

情况二.存在 $b \in G \setminus H$, 且 $b^2 \in \mho_1(H)$.

不妨设 $b^2 = a_1^2$. 此时 $(ba_1)^2 = [a_1, b] \neq a_1^2$. 以下断言 $l = 2$.

若否, 有 $l = 1$ 或 $l > 2$.

当 $l = 1$ 时, 令 $\overline{H} = \langle ba_1, a_1^2, C\rangle$, 则 $\overline{H}$ 也是 G 的最大阶的交换子群. 若对所有的 $d \in G \setminus \overline{H}$, $d^2 \notin \mho_1(\overline{H})$, 可转化为情况一. 若存在 $d \in G \setminus \overline{H}$, 且 $d^2 \in \mho_1\overline{H})$. 即 $d^2 = (ba_1)^2 \neq b^2 = a_1^2$. 由引理 5.1.4(2) 及断言 (1) 有 $[a_1, d] = a_1^2$ 或 $[a_1, d] = d^2$, 此时断言此情况不存在. 以下我们分情况推出矛盾:

当 $[a_1, d] = a_1^2 = b^2$ 时, 若 $[b, d] = 1$, 则 $\langle b, d, C\rangle$ 为交换群, 与 H 的最大性矛盾. 所以 $[b, d] \neq 1$. 又由 5.1.4 可知, $[b, d] = b^2$ 或者 $[b, d] = d^2$. 若 $[b, d] = b^2$,

则 $[ba_1, d] = 1$, 从而 $\langle \overline{H}, d \rangle$ 为交换群, 与 H 的最大性矛盾; 若 $[b, d] = d^2$ 时, 因为 $[a_1 d, b] = 1$, $\langle b, a_1 d, C \rangle$ 也为交换群, 也与 H 的最大性矛盾.

当 $[a_1, d] = d^2$ 时, 同理有 $[b, d] = b^2$ 或者 d^2. 若 $[b, d] = b^2$, 由 $[bd, a_1] = 1$, 可知 $L = \langle \overline{H}, bd \rangle$ 为交换群, 这与 $\overline{H}$ 的最大性矛盾; 若 $[b, d] = d^2$, 则 $[ba_1, d] = 1$, $\langle ba_1, d, C \rangle$ 为交换群, 与 H 的最大性矛盾.

故 $l > 2$. 首先断言: $[a_1, b] \in \mho_1(H)$.

因为 $b^2 = a_1^2 \neq a_2^2$, 由断言 1 和引理 5.1.4(2) 有 $[a_2, b] = b^2$ 或 a_2^2 同理 $[a_1 a_2, b] = a_1^2$ 或 $(a_1 a_2)^2$. 从而 $[a_1, b] = a_2^2$ 或 $(a_1 a_2)^2$.

因为 $l > 2$, 同理有 $[a_1, b] = a_3^2$ 或 $(a_1 a_3)^2$, 矛盾. 所以断言成立.

不妨设 $[a_1, b] = a_2^2$, 此时 $[a_2, b] = a_1^2$. (若否, 前面证明过程有 $[a_2, b] = a_2^2$, 考虑 $[a_1 a_2, b] = 1$, 与断言 (1) 矛盾.)

此时若 $G = \langle H, b \rangle$, 即 G 为定理中 (2) 型群.

若 $G \neq \langle H, b \rangle$, 取 $d \in G \setminus \langle H, b \rangle$, 断言 $d^2 \in \mho_1(H) = \{\alpha_1^2, a_2^2, (a_1 a_2)^2\}$. 若否, 由引理 5.1.4(2) 及断言 (1) 可知, $[a_1, d] = a_1^2$ 或 d^2, $[a_2, d] = a_2^2$ 或 d^2, 容易证明 $[a_1, d] = a_1^2$, $[a_2, d] = a_2^2$(考虑 $[a_1 a_2, d]$), 此时再考虑 $[a_1 a_2, bd] = [a_1 a_2, d][a_1 a_2, b] = 1$, 与断言 (1) 矛盾, 故断言成立.

任取 $d \in G \setminus \langle H, b \rangle$, 最后我们分三种情况讨论:

情况 (1). $d^2 = a_2^2$,

由引理 5.1.4(2) 及断言 1 可知, $[a_1, d] = a_1^2$ 或 a_2^2, $[a_1 a_2, d] = (a_1 a_2)^2$ 或者 a_2^2.

这迫使 $[a_2, d] = a_1^2$ 或者 $(a_1 a_2)^2$, 若 $[a_2, d] = a_1^2$, 考虑 $[a_2, bd] = [a_2, b] a_1^2 = 1$, 与断言 (1) 矛盾. 所以 $[a_2, d] = (a_1 a_2)^2$, 此时必有 $[a_1, d] = a_1^2$.

我们断言 $G = \langle H, b, d \rangle$. 若否, 则存在 $f \in G \setminus \langle H, b, d \rangle$. 由前面证明过程可得出 $f^2 \in \mho_1(H) = \{\alpha_1^2, a_2^2, (a_1 a_2)^2\}$. 若 $f^2 = a_2^2$, 由断言 1 和 5.1.4(2) 可知, $[a_1, f] = a_1^2$ 或者 a_2^2, 此时分别有 $[a_1, df] = 1$ 和 $[a_1, bf] = 1$, 这都与断言 1 矛盾; 若 $f^2 = a_1^2$ 或者 $a_1^2 a_2^2$, 用同样的方法也可推出矛盾.

因为 $b^2 \neq d^2$, 由引理 5.1.4(2) 可得 $[b, d] = 1, b^2, d^2$.

若 $[b, d] = b^2$, 则 $\langle a_2, bd \rangle \cong Q_8$, 与 G 为 T_4 群矛盾.

若 $[b, d] = 1$, 则 G 为定理中 (3) 型群.

若 $[b, d] = d^2$, 用 $a_1 d$ 代替 d 即为定理中 (3) 型群.

情况 (2). $d^2 = a_1^2$,

由断言 1 和 5.1.4(2) 可知, $[a_2, d] = a_1^2$ 或者 a_2^2, 同理 $[a_1a_2, d] = (a_1a_2)^2$ 或者 a_1^2. 这迫使 $[a_1, d] = (a_1a_2)^2$ 或者 a_2^2. 若 $[a_1, d] = a_2^2$, 则必有 $[a_2, d] = a_1^2$ 此时 $[a_1, bd] = 1$, 与断言 1 矛盾. 所以 $[a_1, d] = (a_1a_2)^2$, 此时 $[a_2, d] = a_2^2$.

考虑子群 $B = \langle a_2, bd\rangle$. 因为 $[a_2, bd] = (a_1a_2)^2 \neq 1$, 所以 $B \cong M_{2,2,2}$, 从而 $[b, d] = (bd)^2 \in \Phi(B) = \langle a_1^2, a_2^2\rangle$. 易知 $(bd)^2 \neq 1, a_1^2$. 若 $(bd)^2 = a_2^2$, 用 bd 代替 d 可转化为情况 1; 若 $(bd)^2 = (a_1a_2)^2$, 则 $(a_2bd)^2 = a_2^2$, 用 a_2bd 代替 d 即可转化为情况 (1).

情况 (3). $d^2 = a_1^2a_2^2$.

由断言 1 和 5.1.4(2) 可知, $[a_1, d] = a_1^2$ 或者 $a_1^2a_2^2$, $[a_2, d] = a_1^2a_2^2$ 或者 a_2^2. 这迫使 $[a_1a_2, d] = a_1^2$ 或者 a_2^2. 若 $[a_1a_2, d] = a_1^2$, 则有 $[a_1, d] = a_1^2a_2^2$, 此时 $(a_1d)^2 = a_1^2$. 用 a_1d 替换 d 可转化为情况 2; 若 $[a_1a_2, d] = a_2^2$, 则有 $[a_2, d] = a_1^2a_2^2$, 此时 $(a_2d)^2 = a_2^2$. 用 a_2d 替换 d 可转化为情况 (1).

由定理的证明过程可知, 定理中 (1) 型群与 (2) 型群和 (3) 型群不同构. 而 (2) 型群和 (3) 型群的阶不同, 故它们也不同构.

再证定理中群为 T_4 群: 由定理 5.1.1(7) 可知, 只需证 H 为 T_4 群即可. 以下分情况讨论:

情况 1: (1) 型群.

对任意的 $x, y \in H$, 由 $b^2 \in \Omega_1(H) = Z(H)$. 若 $[x, y] \neq 1$, 从而不妨设 $x = n_1b$, $y = n_2b$, 其中 $n_1, n_2 \in K$, 考虑 $L = \langle x, y\rangle$, $[x, y] = [n_1b, n_2b] = n_1^{-2}n_2^2 = (n_1^{-1}n_2)^2 = (yx^{-1})^2 \neq 1$. 又因为 $L = \langle yx^{-1}, x\rangle$, 所以 $L \cong M_{2,2,2}$. 由 x, y 的任意性, H 为 T_4 群.

情况 2: (2) 型群.

对任意的 $x, y \in H$, 由 $b^2 \in \Omega_1(H) = Z(H)$. 若 $[x, y] \neq 1$, 从而不妨设 $x = a_1^{i_1}a_2^{i_2}b$, $y = a_1^{j_1}a_2^{j_2}b$, 考虑 $L = \langle x, y\rangle$, $[x, y] = [a_1^{i_1}a_2^{i_2}b, a_1^{j_1}a_2^{j_2}b] = (a_1^{i_2-j_2}a_2^{i_1-j_1})^{-2} \neq 1$, $x^2 = a_1^{2(i_1+i_2)}a_2^{2(i_1+i_2)}b^2$, $y^2 = a_1^{2(j_1+j_2)}a_2^{2(j_1+j_2)}b^2$, 此时必有 $o([x, y]) = 2$, $o(x) = o(y) = 4$, 从而可知 L 为内交换群. 由 $[x, y] = (a_1^{i_2-j_2}a_2^{i_1-j_1})^{-2} \neq 1$, 分情况讨论: (1)$i_2 - j_2 \equiv 0 (\mathrm{mod}\ 2)$, $i_1 - j_1 \equiv 1 (\mathrm{mod}\ 2)$, (2)$i_2 - j_2 \equiv 1 (\mathrm{mod}\ 2)$, $i_1 - j_1 \equiv 0 (\mathrm{mod}\ 2)$. (3)$i_2 - j_2 \equiv 1 (\mathrm{mod}\ 2)$, $i_1 - j_1 \equiv 1 (\mathrm{mod}\ 2)$

当 $i_2 - j_2 \equiv 0 \pmod 2$, $i_1 - j_1 \equiv 1 \pmod 2$ 时, 我们有 $i_1 + i_2 \equiv 1 + j_1 + j_2 \pmod 2$. 且通过计算可得: 当 $j_1 + j_2 \equiv 0 \pmod 2$ 时, $[x, y] = x^2$; 当 $j_1 + j_2 \equiv 1 \pmod 2$ 时, $[x, y] = y^2$. 易知 $L \cong M_{2,2,2}$.

当 $i_2 - j_2 \equiv 1 \pmod 2$, $i_1 - j_1 \equiv 0 \pmod 2$ 或 $i_2 - j_2 \equiv 1 \pmod 2$, $i_1 - j_1 \equiv 1 \pmod 2$ 时, 类似于上面的证明过程也可知 $L \cong M_{2,2,2}$. 由 x, y 的任意性, H 为 T_4 群.

情况 3: (3) 型群.

对任意的 $x, y \in H$. 由 $b^2, a_1^2, a_2^2 \in \Omega_1(H) = Z(H)$, 从而不妨设 $x = a_1^{i_1} a_2^{i_2} bd$, $y = a_1^{j_1} a_2^{j_2} bd$. 考虑 $L = \langle x, y \rangle$. 若 $[x, y] = [a_1^{i_1} a_2^{i_2} bd, a_1^{j_1} a_2^{j_2} bd] = (a_1^{i_1 - j_1} a_2^{i_1 + i_2 - j_1 - j_2})^2 \neq 1$, 用类似于 (2) 型群的方法讨论可知 $L \cong M_{2,2,2}$. 又由 x, y 的任意性, H 为 T_4 群. □

定理 5.1.6. 设 $p > 2$. 有限 p 群 G 为非交换的 T_4 群, 若 G 所有的二元生成的非交换子群均同构于 $M_{2,2,p}$, 则:

$G \cong H \times C_p^m$, 其中 $H = K \rtimes \langle b \rangle$ 是 $K = \langle a_1 \rangle \times \langle a_2 \rangle \times \ldots \langle a_k \rangle \cong C_{p^2}^k$ 被 $\langle b \rangle$ 的循环扩张, 满足 $o(b) = p^2$,$a_i^b = a_i^{1+p}$, 对 $1 \leqslant i \leqslant k$ 成立.

证明: 令 $H_m = K \rtimes \langle b \rangle$, 其中 $K = \langle a_1 \rangle \times \langle a_2 \rangle \times \ldots \langle a_m \rangle \cong C_{p^2}^m$, $o(b) = p^2$, $a_i^b = a_i^{1+p}$, 对任意的 $1 \leqslant i \leqslant m$. 由题设存在 G 的子群 $H_1 = \langle a, b \mid a^{p^2} = b^{p^2} = 1, [a, b] = a^p \rangle \cong M_{2,2,p}$. 取 $H = H_k$ 是 G 的子群满足 k 最大.

首先断言: $\mho_1(G) = \mho_1(H) = \Omega_1(H)$. 类似于引理 5.1.4(1) 的证明过程有 $\exp(G) = p^2$, 只需证对任意的 $g \in G$, $g^p \in H$. 若否, 存在 $g \in G$, 使得 $g^p \notin H$. 对任意的 $a \in K \backslash \mho_1(K)$, 若 $[a, g] \neq 1$, 由题设 $\langle a, g \rangle \cong M_{2,2,p}$. 所以无论 $\langle a, g \rangle$ 是否交换, 均可令 $[a, g] = a^{ip} g^{jp}$. 若 $(j, p) = 1$, 此时 $[a, bg] = a^{(1+ip)} g^{jp} \neq 1$. 由题设 $\langle a, bg \rangle \cong M_{2,2,p}$. 此时 $\mho_1(\langle a, bg \rangle) \geqslant \langle a^p, b^p, g^p \rangle \cong C_p^3$, 矛盾. 故可令 $[a_l, g] = a_l^{i_l p}$, 其中 $1 \leqslant l \leqslant k$, $0 \leqslant i_l \leqslant p - 1$. 若 $i_1 \neq i_2$, 考虑 $[a_1 a_2, g] = a_1^{i_1 p} a_2^{i_2 p} \neq 1$, 由题设 $\langle a_1 a_2, g \rangle \cong M_{2,2,p}$. 此时 $\mho_1(\langle a_1 a_2, g \rangle) \geqslant \langle a_1^p, a_2^p, g^p \rangle \cong C_p^3$, 矛盾. 所以有 $i_1 = i_2$. 同理可知 $i_1 = i_2 = \cdots = i_k$. 令 $a_{k+1} = g b^{-i_1}$, 此时 $[a_1, a_{k+1}] = 1$ 且 $a_{k+1}^p \notin H$. 若 $[a_{k+1}, b] \neq 1$, 由题设 $\langle a_{k+1}, b \rangle \cong M_{2,2,p}$. 所以无论 $[a_{k+1}, b] = 1$ 与否, 均有 $[a_{k+1}, b] \in \langle a_{k+1}^p, b^p \rangle$. 同理可得 $[a_{k+1}, b] = [a_{k+1}, a_1 b] \in \langle a_{k+1}^p, a_1^p b^p \rangle$. 从而有 $[a_{k+1}, b] \in \langle a_{k+1}^p \rangle$. 令

$[a_{k+1}, b] = a_{k+1}^{sp}$, 其中 $0 \leqslant s \leqslant p-1$. 若 $s=1$, 则 $\langle H, a_{k+1}\rangle \cong H_{k+1}$, 与 k 的取法矛盾; 若 $s \neq 1$, 令 $T = \langle a_1 a_{k+1}, b\rangle$. 因为 $[a_1 a_{k+1}, b] = a_1^p a_{k+1}^{sp} \neq 1$, 从而由题设有 $T \cong M_{2,2,p}$. 此时因为 $\Phi(T) \geqslant \langle a_1^p a_{k+1}^p, b^p, a_1^p a_{k+1}^{sp}\rangle = \langle a_1^p, a_{k+1}^p, b^p\rangle$, $|\Phi(T)| \geqslant p^3$, 矛盾. 从而断言成立.

由题设可知, 对任意的 $u, v \in G$, 其中 $[u,v] \neq 1$, $[u,v] \in \Phi(\langle u,v\rangle) = \mho_1(\langle u,v\rangle) \leqslant H$. 从而有 $H \trianglelefteq G$. 可令 $G/H = \langle \bar{y_1}, \bar{y_2}, \ldots, \bar{y_n}\rangle$. 由前面的断言可知, 存在 $h_i \in H$ 使得 $y_i^p = h_i^p$. 令 $x_i = y_i h_i^{-1}$. 从而 $x_i^p = 1$ 且 $G/H = \langle \bar{x_1}, \bar{x_2}, \ldots, \bar{x_n}\rangle$. 令 $E = \langle x_1, x_2, \ldots, x_n\rangle$. 由定理 5.1.1 可知, $E \leqslant \Omega_1(G)$ 为初等交换群. 从而 $G = H \times E$.

再证定理中群为 T_4 群: 由定理 5.1.1(7) 可知, 只需证 $H = K \rtimes \langle b\rangle$ 为 T_4 群即可. 对任意的 $x, y \in H$, 可设 $x = n_1 b^i$, $y = n_2 b^j$, 其中 $n_1, n_2 \in K$, 考虑 $L = \langle x, y\rangle$, 若 $[x,y] = [n_1 b^i, n_2 b^j] = n_1^{jp} n_2^{-ip} = (n_1^j n_2^{-i})^p = (x^j y^{-i})^p \neq 1$, 用 $x^j y^{-i}$ 替换 x 或 y, 从而 $L \cong M_{2,2,p}$. 由 x, y 的任意性, H 为 T_4 群. □

定理 5.1.7. *G 为非交换的 T_4 群, 且 G 的所有的非交换二元生成子群均同构于 $N_{2,1,2}$. 设 G 有子群 $H = \langle a, b \mid a^4 = b^2 = c^2 = 1, [a,b] = c, [c,a] = [c,b] = 1\rangle \cong N_{2,1,2}$, 则:*

(1) $\exp G = 2^2$;

(2) $C_G\langle a\rangle = \langle a\rangle \times C$, 其中 C 为初等交换 2 群;

(3) 对任意的 $y \in G \setminus C_G(a)$, 存在 2 阶元 x 使得 $xC_G(a) = yC_G(a)$.

证明: (1)(反证法) 若否, 由定理 5.1.1 则 $\exp G = 2^3$. 即存在 $g \in G$, 使得 $o(g) = 2^3$. 从而 $g \in Z(G)$. 同理 $o(bg) \in Z(G)$, 进而 $b \in Z(G)$, 与 $[a,b] \neq 1$ 矛盾.

(2) 我们首先证明 $C_G\langle a\rangle$ 为交换群. 若否, 存在 $K = \langle x, y \mid x^4 = y^2 = z^2 = 1, [x,y] = z, [z,x] = [z,y] = 1\rangle \cong N_{2,1,2}$ 为 $C_G\langle a\rangle$ 的子群. 考虑 $M = \langle x, ay\rangle$, $[x, ay] = [x,y] = z \neq 1$, 由内交换群的结构可知 $z \in \langle x^2, a^2\rangle = \Phi(M)$(显然 $a^2 \neq x^2$, 若否, 考虑 $\langle ax, b\rangle$). 又由 G 为 T_4 群可知 $z = x^2a^2 = (ax)^2$, 再考虑 $\langle ax, y\rangle$, $[ax, y] = [x,y] = z = (ax)^2$, 故 $\langle ax, y\rangle \cong D_8$, 与 G 为 T_4 群矛盾.

故 $C_G\langle a\rangle$ 为交换群. 又因为 $\exp(C_G\langle a\rangle) = 2^2$, 所以存在子群 C 使得 $C_G\langle a\rangle = \langle a\rangle \times C$.

以下我们证明 C 为初等交换 2 群. 若否, 存在 $a_1 \in C$ 为 4 阶直积因子. 若 $[b, a_1] = 1$, 考虑 $\langle a, ba_1 \rangle$, 类似于 (2) 的证明可知 $[a, ba_1] = c = a^2 a_1^2 = (aa_1)^2$, 再考虑 $\langle aa_1, b \rangle$, $[aa_1, b] = c = (aa_1)^2$. 故 $\langle aa_1, b \rangle \cong D_8$, 与 G 为 $\mathcal{T}_4$ 群矛盾. 故 $[b, a_1] \neq 1$. 断言 $[b, a_1] = c$. 若否, 令 $[b, a_1] = m \neq c$. 考虑 $\langle ab, a_1 \rangle$, $[ab, a_1] = m = a^2 c a_1^2 = (aa_1)^2 c$. 即 $(aa_1)^2 = mc$. 再考虑 $\langle aa_1, b \rangle$, $[aa_1, b] = cm = (aa_1)^2$. 故 $\langle aa_1, b \rangle \cong D_8$. 与 G 为 $\mathcal{T}_4$ 群矛盾. 故 $[b, a_1] = c$. 考虑 $\langle ab, a_1 \rangle$, $[ab, a_1] = [b, a_1] = c = a^2 c a_1^2$. 即 $a^2 a_1^2 = 1$. 矛盾.

故 C 为初等交换 2 群.

(3) 因为 $y \notin C_G\langle a \rangle$, 所以 $Q = \langle a, y \rangle \cong N_{2,1,2}$. 不妨设 $Q = \langle a, b \mid a^4 = b_1^2 = c_1^2 = 1, [a, b_1] = c_1, [b_1, c_1] = [a, b_1] = 1 \rangle$, 则可设 $y = a^i b_1^j c_1^k$, 其中 $(j, 2) = 1$. 令 $x = b_1^j$, 则有 $xC_G(a) = yC_G(a)$. □

定理 5.1.8. 设 G 为非交换的 $\mathcal{T}_4$ 群, 若 G 所有的二元生成的非交换子群均同构于 $N_{2,1,2}$, 则:

$G \cong H \times C_2^n$. 其中 $H = K \rtimes \langle a \rangle$, 是 $K = \langle b_1 \rangle \times \langle b_2 \rangle \times \cdots \times \langle b_k \rangle \times \langle c_1 \rangle \times \langle c_2 \rangle \times \cdots \times \langle c_k \rangle \cong C_2^{2k}$ 被 $\langle a \rangle$ 的循环扩张, 满足 $a^{2^2} = 1$, $b_i^a = b_i c_i^{-1}$, $c_i^a = c_i$ 对任意的 $1 \leqslant i \leqslant k$ 都成立.

证明: 由题设, 存在 $a, b_1 \in G$, 使得 $\langle a, b_1 \mid a^4 = b_1^2 = c_1^2 = 1, [a, b_1] = c_1, [c_1, a] = [c_1, b_1] = 1 \rangle \cong N_{2,1,2}$, 由定理 5.1.1(6) 可知 $C_G(a) \trianglelefteq G$. 设 $G/C_G(a) = \langle \bar{y_1}, \bar{y_2}, \cdots, \bar{y_m} \rangle$, 由引理 5.1.7, 存在 2 阶元 $x_1, x_2, \cdots, x_m$ 使得 $G/C_G(a) = \langle \bar{x_1}, \bar{x_2}, \cdots, \bar{x_m} \rangle$, 设 $M = \langle x_1, x_2, \cdots, x_m \rangle$ 则由定理 5.1.1(3) 可知 $M \leqslant \Omega_1(G)$ 是交换群. 设 $M = (M \cap C_G(a)) \times N$, 则 $G = C_G(a)M = C_G(a) \times N$, 设 φ 是从 N 到 $C_G(a)$ 的映射, 满足 $\varphi(n) = [a, n]$, 对任意的 $n \in N$. 由 $N \cap C_G(a) = 1$ 可知 φ 是单射, 即 $[a, N] = \varphi(N) \cong N$. 又由 G 为 $\mathcal{T}_4$ 群可知 2^3 阶群都交换, 故 $[a, N] \cap \langle a \rangle = 1$, 从而 $\langle a \rangle \times [a, N]$ 是 $C_G(a)$ 的直积因子. 设 $N = \langle b_1 \rangle \times \langle b_2 \rangle \times \cdots \times \langle b_k \rangle$ $[a, b_i] = c_i$, 其中 $1 \leqslant i \leqslant k$, 则 $G' = [a, N] = \langle c_1 \rangle \times \langle c_2 \rangle \times \cdots \times \langle c_k \rangle$. 令 $K = N \times G'$, 则 $H = K \rtimes \langle a \rangle$ 满足 $a^{2^2} = 1$, $b_i^a = b_i c_i^{-1}$, $c_i^a = c_i$ 对任意的 $1 \leqslant i \leqslant k$ 都成立. 再设 $C_G(a) = \langle a \rangle \times G' \times E$, 则 E 为初等交换 2 群. 从而 $G = (K \rtimes \langle b \rangle) \times E$.

再证定理中群为 $\mathcal{T}_4$ 群: 要证明 G 为 $\mathcal{T}_4$ 群, 由定理 5.1.1(7) 可知, 只需证明 $H = K \rtimes \langle a \rangle$ 为 $\mathcal{T}_4$ 群即可.

由 H 的结构可知，H 中任一元素均可写成 $b_1^{j_1}b_2^{j_2}\cdots b_k^{j_k}a^{i_1}c_1^{l_1}\cdots c_k^{l_k}$. 又因为 $c_i\in Z(H)$. 且 $o(c_i)=2$. 对任意的 $x,y\in H$, 不妨设 $x=b_1^{j_1}b_2^{j_2}\cdots b_k^{j_k}a^{i_1}$, $y=b_1^{j_1'}b_2^{j_2'}\cdots b_k^{j_k'}a^{i_1'}$, 考虑 $L=\langle x,y\rangle$, 若 $[x,y]=c_1^{i_1j_1'-i_1'j_1}c_2^{i_1j_2'-i_1'j_2}\cdots c_k^{i_1j_k'-i_1'j_k}\neq 1$. 从而 i_1,i_1' 不能同时同余于 0 模 2. 从而 L 为内交换群. 若 $(i_1,2)=1,(i_1',2)=1$, 此时 $L=\langle x,xy\rangle\cong N_{2,1,2}$, 若 i_1,i_1' 有一个同余于 0 模 2, 显然 $L=\langle x,y\rangle\cong N_{2,1,2}$. 故 H 满足定理中的条件. □

引理 5.1.9. *设 $p>2$, 有限 p 群 G 为非交换的 T_4 群, 且 G 所有的二元生成的非交换子群均同构于 $N_{2,1,p}$. 设 G 有子群 $H=\langle a,b\mid a^{p^2}=b^p=c^p=1,[a,b]=c,[c,a]=[c,b]=1\rangle\cong N_{2,1,p}$, 则:*

(1) $\exp G=p^2$;

(2) $C_G\langle a\rangle=\langle a\rangle\times C$, *其中 C 为初等交换 p 群;*

(3) *对任意的 $y\in G\setminus C_G(a)$, 存在 p 阶元 x 使得 $xC_G(a)=yC_G(a)$.*

证明: (1)(反证法) 若否, 由定理 5.1.1 则 $\exp G=p^3$. 即存在 $g\in G$, 使得 $o(g)=p^3$. 由内交换群的结构可知, $g\in Z(G)$, 同理 $o(bg)\in Z(G)$, 进而 $b\in Z(G)$, 与 $[a,b]\neq 1$ 矛盾.

(2) 我们首先证明 $C_G\langle a\rangle$ 为交换群. 若否, 存在 $K=\langle x,y\mid x^{p^2}=y^p=z^p=1,[x,y]=z,[z,x]=[z,y]=1\rangle\cong N_{2,1,p}$, 为 $C_G\langle a\rangle$ 的子群. 考虑 $M=\langle x,ay\rangle$. $[x,ay]=[x,y]=z\neq 1$, 故 $M\cong N_{2,1,p}$. 由内交换群的结构可知 $\Phi(M)=\langle x^p,z\rangle$. 又由于 $a^p=(ay)^p\in\Phi(M)$, 可设 $a^p=x^{ip}$. 再考虑子群 $N=\langle ax^{-i},y\rangle$, 由 $\langle ax^{-i}\rangle\trianglelefteq G$ 可知 $|N|\leqslant p^3$, 由 G 为非交换的 T_4 群可知 N 交换, 即 $a^p=z^j$(显然 (j,p)=1). $\mho_1(M)=\langle x^p,a^p\rangle=\Phi(M)$, 与内交换群的结构矛盾.

故 $C_G\langle a\rangle$ 为交换群. 又因为 $\exp(C_G\langle a\rangle)=p^2$, 所以存在子群 C 使得 $C_G\langle a\rangle=\langle a\rangle\times C$.

以下我们证明 C 为初等交换 p 群. 若否, 存在 $a_1\in C$ 为 p^2 阶元. 若 $[b,a_1]=1$, 考虑 $L=\langle a,ba_1\rangle$, $[a,ba_1]=c\neq 1$, 故 L 非交换且 $\Phi(L)=\mho_1(L)=\langle a^p,a_1^p\rangle$, 与内交换群的结构矛盾. 故 $[b,a_1]\neq 1$, 此时由题设可知 $\langle ab,a_1\rangle\cong N_{2,1,p}$, 由内交换群的结构 (3) 可知 $\langle (ab)^p\rangle=\langle a_1^p\rangle$ 与 $\langle a\rangle\cap C=1$ 矛盾. 故 C 为初等交换 p 群.

(3) 因为 $y \notin C_G\langle a\rangle$, 所以 $Q=\langle a,y\rangle \cong N_{2,1,2}$. 不妨设 $Q=\langle a,b \mid a^{p^2}=b_1^p=c_1^p=1,[a,b_1]=c_1,[b_1,c_1]=[a,b_1]=1\rangle$, 则可设 $y=a^ib_1^jc_1^k$, 其中 $(j,p)=1$. 令 $x=b_1^j$, 则有 $xC_G(a)=yC_G(a)$. □

定理 5.1.10. 设 $p>2$, 有限 p 群 G 为非交换的 T_4 群. 若 G 所有的二元生成的非交换子群均同构于 $N_{2,1,p}$, 则:

$G\cong H\times C_p^n$. 其中 $H=K\rtimes\langle a\rangle$, 是 $K=\langle b_1\rangle\times\langle b_2\rangle\times\cdots\times\langle b_k\rangle\times\langle c_1\rangle\times\langle c_2\rangle\times\cdots\times\langle c_k\rangle\cong C_p^{2k}$ 被 $\langle a\rangle$ 的循环扩张, 满足 $a^{p^2}=1$, $b_i^a=b_ic_i^{-1}$, $c_i^a=c_i$ 对任意的 $1\leqslant i\leqslant k$ 都成立.

证明: 由题设, 存在 $a,b_1\in G$, 使得 $\langle a,b_1 \mid a^{p^2}=b_1^p=c_1^p=1,[a,b_1]=c_1,[c_1,a]=[c_1,b_1]=1\rangle\cong N_{2,1,p}$. 由定理 5.1.1(6) 可知 $C_G(a)\trianglelefteq G$. 设 $G/C_G(a)=\langle\bar{y_1},\bar{y_2},\cdots,\bar{y_m}\rangle$, 由引理 5.1.7, 存在 p 阶元 $x_1,x_2,\cdots,x_m$ 使得 $G/C_G(a)=\langle\bar{x_1},\bar{x_1},\cdots,\bar{x_1}\rangle$, 设 $M=\langle x_1,x_2,\cdots,x_m\rangle$ 则由定理 5.1.1(3) 可知 $M\leqslant\Omega_1(G)$ 是交换群. 设 $M=(M\cap C_G(a))\times N$, 则 $G=C_G(a)M=C_G(a)\times N$, 设 φ 是从 N 到 $C_G(a)$ 的映射, 满足 $\varphi(n)=[a,n]$, 对任意的 $n\in N$. 由 $N\cap C_G(a)=1$ 可知 φ 是单射, 即 $[a,N]=\varphi(N)\cong N$. 又由 G 为 T_4 群可知 p^3 阶群都交换. 故 $[a,N]\cap\langle a\rangle=1$, 从而 $\langle a\rangle\times[a,N]$ 是 $C_G(a)$ 的直积因子. 设 $N=\langle b_1\rangle\times\langle b_2\rangle\times\cdots\times\langle b_k\rangle$, $[a,b_i]=c_i$, 其中 $1\leqslant i\leqslant k$, 则 $G'=[a,N]=\langle c_1\rangle\times\langle c_2\rangle\times\cdots\times\langle c_k\rangle$. 令 $K=N\times G'$, 则 $H=K\rtimes\langle a\rangle$ 满足 $a^{2^2}=1$, $b_i^a=b_ic_i^{-1}$, $c_i^a=c_i$ 对任意的 $1\leqslant i\leqslant k$ 都成立. 再设 $C_G(a)=\langle a\rangle\times G'\times E$, 则 E 为初等交换 p 群. 从而 $G=(K\rtimes\langle b\rangle)\times E$.

再证定理中群为 T_4 群: 同理只需证明 H 为 T_4 群即可. 对任意的 $x,y\in H$, 令 $x=b_1^{i_1}b_2^{i_2}\cdots b_k^{i_k}ca^m$, $y=b_1^{j_1}b_2^{j_2}\cdots b_k^{j_k}c'a^n$, 其中 $c,c'\in\langle c_1\rangle\times\langle c_2\rangle\times\cdots\times\langle c_k\rangle\cong C_p^k$. 则

$$
\begin{aligned}
[x,y] &= [b_1^{i_1}b_2^{i_2}\cdots b_k^{i_k}ca^m, b_1^{j_1}b_2^{j_2}\cdots b_k^{j_k}c'a^n] \\
&= c_1^{i_1m}c_2^{i_2m}\cdots c_k^{i_km}c_1^{-j_1n}c_2^{-j_2m}\cdots c_k^{i_km}
\end{aligned}
$$

若 $[x,y]\neq 1$, 显然 $L=\langle x,y\rangle$ 为内交换群, 且 m,n 不能同时同余于零模 p.

若 $m|p$, 或 $n|p$, 此时显然 $L=\langle x,y\rangle\cong N_{2,1,p}$. 若 $(m,p)=1$, 且 $(n,p)=1$, 此时有 $x^p=a^{mp}$, $y^p=a^{np}$, 从而 $\langle x^p\rangle=\langle y^p\rangle$, 即存在 l 使得 $(l,p)=1$, 且 $x^p=y^{lp}$, 此时 $L=\langle x,y\rangle=\langle x,xy^{-l}\rangle\cong N_{2,1,p}$. 故 G 为满足条件的群. □

引理 5.1.11. 设 G 为非交换的 T_4 群. 若 G 有两个二元生成的非交换子群同构于 $M_{2,2,p}$ 和 $N_{2,1,p}$, 且无子群同构于 $M_{3,1,p}$. 设 G 的子群 H 满足 H 的任意非交换的二元生成子群全同构于 $N_{2,1,p}$, 并且 H 的阶最大. 则可设 $H = (K \rtimes \langle b\rangle)\times E$, 其中 $K = \langle a_1\rangle\times\langle a_2\rangle\times\cdots\times\langle a_k\rangle\times\langle c_1\rangle\times\langle c_2\rangle\times\cdots\times\langle c_k\rangle\cong C_p^{2k}$, E 为初等交换 p 群, $a_i^b = a_ic_i, c_i^b = c_i$ 对任意的 $1\leqslant i\leqslant k$. 则:

(1) 对任意的 $d\in G\setminus H$, $d^p\in\langle b^p, c_i\rangle\setminus\{1\}$, 对任意的 $1\leqslant i\leqslant k$ 成立;

(2) $k=1$;

(3) 当 $p=2$ 时, 对任意的 $x\in G\setminus H$, 存在 $h\in H$ 使得 $d = xh$ 满足下列三组关系之一:

(i) $d^2 = c_1, [a_1, d] = [b, d] = 1;$

(ii) $d^2 = c_1, [b, d] = 1, [a_1, d] = b^2c_1;$

(iii) $d^2 = c_1, [b, d] = b^2, [a_1, d] = b^2.$

(4) $E\leqslant Z(G)$.

证明: (1) 由定理 5.1.8, 可设 H 为定理所叙.

首先断言: $\Omega_1(G) = \Omega_1(H) = K\times\langle b^p\rangle\times E$. 因为 G 为 T_4 群, 由引理 5.1.1, $\Omega_1(G)$ 为交换群. 又因为 $\Omega_1(G)\trianglelefteq G$, 且 $b^p\in\Omega_1(G)$, 所以 $\Omega_1(G)\lessdot\Omega_1(G)\langle b\rangle$. 任取 $\Omega_1(G)\langle b\rangle$ 的非交换的二元生成子群 L, 我们有 $L\cap\Omega_1(G)\lessdot L$, 从而 $|\Omega_1(L)| = p^3$. 由内交换群的结构可知 $L\cong N_{2,1,p}$. 这就说明了 $\Omega_1(G)\langle b\rangle$ 的非交换子群全为 $N_{2,1,p}$. 由 H 的最大性 $|\Omega_1(G)\langle b\rangle|\leqslant |H|$, 另一方面 $\Omega_1(H)\leqslant\Omega_1(G)$, 两边同乘 $\langle b\rangle$, 即有 $|H|\leqslant|\Omega_1(G)\langle b\rangle|$. 从而有 $\Omega_1(G) = \Omega_1(H) = K\times\langle b^p\rangle\times E$, 即 H 外无 p 阶元.

再证明: 对任意的 $d\in G\setminus H$, $d^p\in\langle b^2, c_i\rangle$, 且 $d^p\neq 1$, 对任意的 $1\leqslant i\leqslant k$. (反证法) 分 $p=2$ 和 $p>2$ 两种情况讨论:

情况 1: $p=2$. 若 $d^2\notin\langle b^2, c_i\rangle$, 则可知 $|d^2, b^2, c_i| = 2^3$,

由题设只能是 (a)$[b, d] = 1$, (b)$\langle b, d\rangle\cong M_{2,2,2}$, (c)$\langle b, d\rangle\cong N_{2,1,2}$.

(a) 当 $[b, d] = 1$, 考虑子群 $A = \langle a_id, b\rangle$, 由 $[a_id, b] = c_i\neq 1$, 故 A 为 2^4 阶非交换子群且 $\Phi(A) = \langle b^2, c_i\rangle$, 从而 $(a_id)^2 = [a_i, d]d^2\in\Phi(A)$. 再考虑子群 $B = \langle a_ib, d\rangle$, 无论 B 交换与否均有 $|B| = 2^4$ 且 $\Phi(B) = \langle(a_ib)^2, d^2\rangle = \langle b^2c_i, d^2\rangle$. 从而 $[a_ib, d] = [a_i, d]\in\Phi(B)$. 又 $d^2\in\Phi(B)$, 从而 $[a_i, d]d^2\in\Phi(B)\cap\Phi(A) =$

$\langle b^2c_i\rangle$, 此时又有 $[a_i,d]d^2\neq 1$. 故 $[a_i,d]=d^2b^2c_i$, 此时 $\langle a_i,bd\rangle\cong D_8$, 与 G 为 $\mathcal{T}_4$ 群矛盾.

(b) 当 $\langle b,d\rangle\cong N_{2,1,2}$ 时, 因为 $o(b)=o(d)=4$, 所以 $[b,d]=b^2d^2$, $(bd)^2=1$, 进一步有 $bd\in\Omega_1(G)\leqslant H$ 和 $d\in H$, 与题设矛盾.

(c) 当 $\langle b,d\rangle\cong M_{2,2,2}$ 时, 由引理 5.1.4(2), $[b,d]=b^2$ 或 d^2.

若 $[b,d]=b^2$, 考虑子群 $A=\langle a_id,b\rangle$, 同样可得 $(a_id)^2=[a_i,d]d^2\in\Phi(A)=\langle b^2,b^2c_i\rangle$. 从而 $[a_i,d]b^2d^2\in\Phi(A)$ 考虑子群 $B=\langle a_ib,d\rangle$, 可得 $[a_ib,d]=[a_i,d]b^2\in\Phi(B)=\langle b^2c_i,d^2\rangle$, $[a_i,d]b^2d^2\in\Phi(B)\cap\Phi(A)=\langle b^2c_i\rangle$. 得 $[a_i,d]=b^2d^2$ 或 d^2c_i. 若 $[a_i,d]=b^2d^2$, 考虑 $\langle a_ib,a_id\rangle$, $[a_ib,a_id]=b^2d^2c_ib^2=d^2c_i\neq 1$, 而 $\Phi(\langle a_ib,a_id\rangle)=\langle b^2,b^2c_i,d^2c_i\rangle\cong C_2^3$, 从而 $|\langle a_ib,a_id\rangle|\neq 2^4$, 与 G 为 $\mathcal{T}_4$ 群矛盾. 若 $[a_i,d]=d^2c_i$, 此时 $\langle a_i,bd\rangle\cong D_8$, 与 G 为 $\mathcal{T}_4$ 群矛盾.

若 $[b,d]=d^2$, 考虑子群 $A=\langle a_id,b\rangle$, 同样可得 $(a_id)^2=[a_i,d]d^2\in\Phi(A)=\langle b^2,d^2c_i\rangle$, 考虑子群 $B=\langle a_ib,d\rangle$, 可得 $[a_ib,d]=[a_i,d]d^2\in\Phi(B)=\langle b^2c_i,d^2\rangle$, 从而 $[a_i,d]d^2\in\Phi(B)\cap\Phi(A)=\langle d^2b^2c_i\rangle$, 又 $[a_i,d]\neq d^2$, 从而得出 $[a_i,d]=b^2c_i$, 此时 $\langle a_i,bd\rangle\cong D_8$, 与 G 为 $\mathcal{T}_4$ 群矛盾.

情况 2: $p>2$.

首先断言 $\langle d^p\rangle\neq\langle b^p\rangle$. 若否, 不妨设 $d^p=b^{kp}$, 即 b^kd^{-1} 为 p 阶元, H 外有 p 阶元与 $\Omega_1(G)=\Omega_1(H)$ 矛盾.

对任意的 $1\leqslant l\leqslant p$, 考虑子群 $A_l=\langle a_i^ld,b\rangle$, 若 A_l 非交换, 则 A_l 为 p^4 阶的内交换群, 又因为 $\mho_1(A_l)=\langle b^p,d^p\rangle$ 为 p^2 阶初等交换群. 易知 $A_l\cong M_{2,2,p}$. 特别的 $[d,b]\neq 1$, 则 $[d,b]\in\Phi(A_0)=\mho_1(A_0)=\langle b^p,d^p\rangle$.

因为 $[a_i^ld,b]=c_i^l[d,b]$, 所以存在 $1\leqslant s\leqslant p-1$, 使得子群 $A_s=\langle a_i^sd,b\rangle$ 不交换, 此时 $[a_i^sd,b]=c_i^s[d,b]\in\Phi(A_s)=\mho_1(A_s)=\langle b^p,d^p\rangle$. 进而 $c_i\in\langle b^p,d^p\rangle=\Phi(A_s)$. 所以 $d^p\in\langle b^p,c_i\rangle=\Phi(A_s)$.

(2)(反证法) 若否, 任取 $d\in G\setminus H$, 由 (1) 可得 $d^p\in\langle b^p,c_1\rangle\cap\langle b^p,c_2\rangle\setminus\{1\}=\langle b^p\rangle\setminus\{1\}$. 若 $p>2$, 设 $d^p=b^{kp}$, 则 $(db^{-k})^p=1$, 与 H 外无 p 阶元矛盾. 若 $p=2$, 则有 $d^2=b^2$. 又因为 $db\notin H$, 同理 $(db)^2=b^2$, 此时 $\langle b,d\rangle\cong Q_8$, 与 G 为 $\mathcal{T}_4$ 群矛盾.

(3) 由 (1) 可得 $x^2\in\{b^2,c_1,b^2c_1\}$. 以下分情况讨论:

情况一: $x^2=c_1$. 此时若 $[b,x]\neq 1$, 则 $\langle b,x\rangle$ 为 16 阶的内交换群. 从而

$[b,x]\in\Phi(\langle b,x\rangle)=\langle b^2,c_1\rangle$. 以下分情况讨论:

子情况 1:若 $[b,x]=1$. 令 $d=x$. 考虑子群 $A=\langle a_1d,b\rangle$. 由 $[a_1d,b]=c_1\neq 1$. 故 A 为 2^4 阶非交换子群且 $\Phi(A)=\langle b^2,c_1\rangle$, 从而 $(a_1d)^2d^2=[a_1,d]\in\Phi(A)=\langle b^2,c_1\rangle$. 此时若 $[a_1,d]=1$. 则有关系组 (i); 若 $[a_1,d]=b^2c_1$. 则有关系组 (ii); 若 $[a_1,d]=c_1$. 则 $\langle a_1,d\rangle\cong D_8$. 与 G 为 T_4 群矛盾; 若 $[a_1,d]=b^2$. 则 $\langle a_1,bd\rangle\cong D_8$, 与 G 为 T_4 群矛盾.

子情况 2:若 $[b,x]=b^2c_1$. 则 $(bx)^2=1$. 从而 $bx\in\Omega_1(G)\leqslant H$. 进而 $x\in H$, 与题设矛盾.

子情况 3:若 $[b,x]=b^2$. 考虑子群 $A=\langle a_1x,b\rangle$. 由 $[a_1x,b]=b^2c_1\neq 1$ 可知 A 为 16 阶的非交换子群且 $\Phi(A)=\langle b^2,c_1\rangle$. 从而 $(a_1x)^2x^2=[a_1,x]\in\Phi(A)=\langle b^2,c_1\rangle$. 此时若 $[a_1,x]=b^2$, 取 $d=x$ 则有关系组 (iii); 若 $[a_1,x]=b^2c_1$, 取 $d=bx$ 则有关系组 (iii); 若 $[a_1,x]=c_1$. 则 $\langle a_1,x\rangle\cong D_8$. 与 G 为 T_4 群矛盾; 若 $[a_1,x]=1$, 则 $\langle a_1,bx\rangle\cong D_8$, 与 G 为 T_4 群矛盾.

子情况 4:若 $[b,x]=c_1$, 考虑子群 $B=\langle a_1b,x\rangle$. 无论 B 交换与否均有 $|B|=2^4$ 且 $\Phi(B)=\langle b^2,c_1\rangle$. 从而 $[a_1b,x]c_1=[a_1,x]\in\langle b^2,c_1\rangle$. 此时若 $[a_1,x]=1$. 令 $x'=a_1x$ 可得 $(x')^2=c_1$ 且 $[b,x']=1$. 从而可以转化成子情况 1; 若 $[a_1,x]=b^2$, 令 $x'=a_1bx$ 可得 $(x')^2=c_1$ 且 $[b,x']=1$, 从而也可以转化成子情况 1; 若 $[a_1,x]=c_1$, 则 $\langle a_1,x\rangle\cong D_8$, 与 G 为 T_4 群矛盾; 若 $[a_1,x]=b^2c_1$, 则 $\langle a_1,bx\rangle\cong D_8$, 与 G 为 T_4 群矛盾.

情况二: $x^2=b^2c_1$. 此时若 $[b,x]\neq 1$ 则 $\langle b,x\rangle$ 为 16 阶的内交换群, 从而 $[b,x]\in\Phi(\langle b,x\rangle)=\langle b^2,c_1\rangle$. 以下分情况讨论:

子情况 1:若 $[b,x]=1$, 令 $x'=bx$, 则 $(x')^2=c_1$, 从而可以转化成情况一.

子情况 2:若 $[b,x]=b^2$, 考虑子群 $A=\langle a_1x,b\rangle$. 由 $[a_1x,b]=b^2c_1\neq 1$ 可知 A 为 16 阶的内交换子群且 $\Phi(A)=\langle b^2,c_1\rangle$, 从而 $(a_1x)^2x^2=[a_1,x]\in\Phi(A)=\langle b^2,c_1\rangle$. 此时若 $[a_1,x]=b^2$. 令 $x'=a_1x$ 可得 $(x')^2=c_1$. 从而可以转化成情况一; 若 $[a_1,x]=b^2c_1$, 则 $\langle a_1,x\rangle\cong D_8$, 与 G 为 T_4 群矛盾; 若 $[a_1,x]=c_1$, 则 $\langle a_1b,x\rangle\cong Q_8$. 与 G 为 T_4 群矛盾; 若 $[a_1,x]=1$, 则 $\langle a_1b,bx\rangle\cong Q_8$, 与 G 为 T_4 群矛盾.

子情况 3:若 $[b,x]=b^2c_1$, 考虑子群 $C=\langle a_1b,bx\rangle$, 无论 $\langle a_1b,bx\rangle$ 交换与否都有 $|\langle a_1b,bx\rangle|=2^4$ 且 $\Phi(C)=\langle b^2,c_1\rangle$, 从而 $[a_1b,bx]b^2=[a_1,x]\in\langle b^2,c_1\rangle$.

此时若 $[a_1, x] = b^2$, 令 $x' = a_1 x$ 可得 $(x')^2 = c_1$, 从而可以转化成情况一; 若 $[a_1, x] = 1$, 则 $\langle a_1 b, x\rangle \cong Q_8$, 与 G 为 T_4 群矛盾. 若 $[a_1, x] = c_1$, 则 $\langle a_1 x, b\rangle \cong Q_8$, 与 G 为 T_4 群矛盾; 若 $[a_1, x] = b^2 c_1$, 则 $\langle a_1, bx\rangle \cong D_8$, 与 G 为 T_4 群矛盾;

子情况 4:若 $[b, x] = c_1$, 则 $(bx)^2 = 1$, 从而 $bx \in \Omega_1(G) \leqslant H$, 与题设矛盾.

情况三: $x^2 = b^2$. 此时由题设 $(bx)^2 = [b, x] \neq b^2$, 令 $x' = bx$, 可转化为情况一或情况二.

(4) 只需证明对任意的 $e \in E$ 和 $x \in G \setminus H$ 有 $[e, x] = 1$ 即可.

情况 1. $p = 2$.

由 (3) 可知, 存在 $h \in H$ 使得 $d = xh$ 满足关系组 (i), (ii) 或 (iii). 又 $(ed)^2 = [e, d]d^2 = [e, d]c_1 \in \{b^2, c_1, b^2 c_1\}$, 从而 $[e, d] \in \{b^2 c_1, 1, b^2\}$. 若 $[e, d] = b^2 c_1$, 对于关系组 (i), (ii) 有 $\langle e, bd\rangle \cong D_8$, 对于关系组 (iii) 有 $\langle e, a_1 d\rangle \cong D_8$, 都与 G 为 T_4 群矛盾; 若 $[e, d] = b^2$, 对 (i) 有 $\langle a_1 e, bd\rangle \cong D_8$; 对 (ii) 有 $\langle e, a_1 d\rangle \cong D_8$; 对 (iii) 有 $\langle e, a_1 bd\rangle \cong D_8$, 也都与 G 为 T_4 群矛盾. 从而一定有 $[e, x] = 1$. 故 $E \leqslant Z(G)$.

情况 2. $p > 2$.

由 (1) 的证明过程可知 $\langle x^p, b^p\rangle = \langle b^p, c_1\rangle$, 以下断言: 对任意的 $h \in H$, 有 $[h, x] \in \langle x^p, b^p\rangle = \langle b^p, c_1\rangle$. 因为 $H = \Omega_1(G)\langle b\rangle$, 所以可设 $h = gb^l$, 其中 $g \in \Omega_1(G)$, $0 \leqslant l \leqslant p-1$. 对任意的 $1 \leqslant l \leqslant p-1$, 考虑子群 $B_l(g) = \langle gb^l, x\rangle$. 若 $B_l(g)$ 非交换, 则 $B_l(g)$ 为 p^4 阶内交换群, 又因为 $\mho_1(B_l(g)) = \langle x^p, b^p\rangle$ 为 p^2 阶初等交换群. 由内交换群的结构可知 $B_l(g) \cong M_{2,2,p}$. 若 $[gb^l, x] \neq 1$, 则 $[gb^l, x] \in \Phi(B_l(g)) = \mho_1(B_l(g)) = \langle x^p, b^p\rangle$. 这就说明对于 $h \notin \Omega_1(G)$ 断言成立. 又因为 $[g, x] = [gb, x][b^{-1}, x] \in \langle x^p, b^p\rangle$. 所以断言对 $h \in \Omega_1(G)$ 也成立.

设 $x^p = b^{tp} c_1^j$, 则 $(j, p) = 1$, 令 $d = b^{-tj^{-1}} x^{j^{-1}}$, 则 $d^p = c_1$. 为了证明 $[e, x] = 1$, 只需证明 $[e, d] = 1$ 即可. 由前面的断言有 $[e, d] = b^{sp} c_1^t$, $[a_1, d] = b^{up} c_1^v$,.

接下来我们证明 $[e, d] = b^{sp}$. 若否, 则 $(t, p) = 1$. 由 $[e, b^s d^t] = (b^{sp} c_1^t))^t = (b^s d^t)^{tp}$ 可知 $\langle e, b^s d^t\rangle$ 为 p^3 阶非交换群, 与 G 为 T_4 群矛盾.

最后, 我们用反证法证明 $[e, d] = 1$. 若否, 则 $(s, p) = 1$. 若 $(v, p) = 1$. 由 $[a_1^s e^{-u}, d] = c_1^{sv} = d^{svp}$ 可得 $\langle a_1^s e^{-u}, d\rangle$ 为 p^3 阶非交换群, 与 G 为 T_4 群矛盾;

若 $[a_1,d]=b^{up}$, 由

$$[a_1^s e^{1-u}, bd] = b^{sp}c_1^s = (bd)^{sp}$$

可得 $\langle a_1^s e^{1-u}, bd\rangle$ 为 p^3 阶非交换群. 也与 G 为 T_4 群矛盾. □

定理 5.1.12. 设 G 为非交换的 T_4 群. 若 G 有两个二元生成的非交换子群同构于 $M_{2,2,2}$ 和 $N_{2,1,2}$, 且无子群同构于 $M_{3,1,2}$. 设 G 的子群 H 满足 H 的任意非交换的二元生成子群全同构于 $N_{2,1,2}$, 并且 H 的阶最大. 则可设 $H=(K\rtimes\langle b\rangle)\times E$. 其中 $K=\langle a_1\rangle\times\langle a_2\rangle\times\cdots\times\langle a_k\rangle\times\langle c_1\rangle\times\langle c_2\rangle\times\cdots\times\langle c_k\rangle\cong C_2^{2k}$, E 为初等交换 2 群, $a_i^b=a_ic_i, c_i^b=c_i$ 对任意的 $1\leqslant i\leqslant k$. 则 G 为下列群之一:

(1) $H_1\times C_2^n$, $H_1=\langle a,b,c \mid a^2=b^4=c^4=1, [a,b]=c^2, [a,c]=[b,c]=1\rangle$, 其中 n 为非负整数;

(2) $H_2\times C_2^m$, $H_2=\langle a,b,c \mid a^2=b^4=c^4=1, [a,b]=c^2, [a,c]=b^2c^2, [b,c]=1,\rangle$, 其中 m 为非负整数.

证明: 由题设 G 必存在子群 H 使得它的任意非交换的二元生成子群全同构于 $N_{2,1,2}$. 不妨设 H 即为满足上述条件的最大阶的子群, 由定理 5.1.8 可设 $H=(K\rtimes\langle b\rangle)\times E$, 其中 $K=\langle a_1\rangle\times\langle a_2\rangle\times\cdots\times\langle a_k\rangle\times\langle c_1\rangle\times\langle c_2\rangle\times\cdots\times\langle c_k\rangle\cong C_2^{2k}$, E 为初等交换 2 群. $a_i^b=a_ic_i, c_i^b=c_i$. 对任意的 $1\leqslant i\leqslant k$.

由引理 5.1.11(1) 的证明过程可知 $\Omega_1(G)=\Omega_1(H)=K\times\langle b^2\rangle\times E$. 又易知 $H\trianglelefteq G$. (对任意的 $h\in H, d\in G$, 由引理 5.1.1 有 $o([h,d])=2$, 从而 $[h,d]\in\Omega_1(G)=\Omega_1(H)\leqslant H$, 即 $H\trianglelefteq G$.)

此时考虑 G/H, 则 G/H 为初等交换 2 群. 设 $G/H=\langle\overline{d_1}\rangle\times\langle\overline{d_2}\rangle\times\cdots\times\langle\overline{d_s}\rangle$.

以下证明 $s=1$. 若否, 由引理 5.1.11(3) 可知, 存在 $d_1', d_2'\in G\setminus H$, 使得 ${d_1'}^2={d_2'}^2=c_1$, 由引理 5.1.11(1) 和 (3) 可知, $(d_1'd_2')^2\in\langle b^2,c_1\rangle\setminus\{1\}$, 且 $[a_1b, d_1d_2]=1, b^2c_1$.

若 $(d_1'd_2')^2=c_1$, 此时 $\langle d_1', d_2'\rangle\cong Q_8$. 若 $(d_1'd_2')^2=b^2$, 此时考虑 $\langle b, d_1'd_2'\rangle$, 同理 $[b, d_1'd_2']=(bd_1'd_2')^2\neq 1, b^2$. 与引理 5.1.11(3) 矛盾. 若 $(d_1'd_2')^2=b^2c_1$, 且 $[a_1b, d_1d_2]=1$, 此时 $(a_1bd_1d_2)^2=1$. 与 $a_1bd_1d_2\in\Omega_1(G)\leqslant H$ 矛盾; 若 $(d_1d_2)^2=b^2c_1$ 且 $[a_1b, d_1d_2]=b^2c_1$, 此时 $\langle a_1b, d_1d_2\rangle\cong Q_8$, 与 G 为 T_4 群矛盾, 故 $s=1$.

从而可令 $G = \langle H, d_1 \rangle$, 由引理 5.1.11(3) 可知 G 为定理中的群 (1), (2).

因为定理中 (1) 型群和 (2) 型群的导群阶不同, 所以 (1) 型群和 (2) 型群不同构.

要证 G 为 $\mathcal{T}_4$ 群. 由定理 5.1.1(7) 可知, 只需证明 H 为 $\mathcal{T}_4$ 群即可. 以下分情况讨论:

情况 1: (1) 型群.

对任意的 $x, y \in H_1$, 由 $b^2, c \in Z(H_1)$, 从而不妨设 $x = a^i c^m b$, $y = a^j c^n b$, 考虑 $L = \langle x, y \rangle$, 若 $[x, y] = [a^i c^m b, a^j c^n b] = c^{2(i-j)} \neq 1$, 即 $(i-j)$ 与 2 互素且 $o(y) = 4$. 又因为 $L = \langle xy^{-1}, y \rangle$, 若 $((m-n), 2) = 1$, 此时 $L \cong M_{2,2,2}$, 若 $(m-n) | 2$, 此时 $L \cong N_{2,1,2}$. 由 x, y 的任意性,H 为 $\mathcal{T}_4$ 群.

情况 2: (2) 型群.

对任意的 $x, y \in H_2$, 若 $[x, y] \neq 1$, 由 $b^2, c \in Z(H_2)$, 从而不妨设 $x = a^i c^m b$, $y = a^j c^n b$, 考虑 $L = \langle x, y \rangle$, $[x, y] = [a^i c^m b, a^j c^n b] = (bc)^{2(in-mj)} c^{2(i-j)} \neq 1$, 又 $x^2 = b^2 c^{2(i+m+mi)}$, $y^2 = b^2 c^{2(j+n+jn)}$. 经计算可知: 当 $in - mj \equiv 0 \pmod 2$, $i - j \equiv 1 \pmod 2$ 时, $[x, y] = x^2 y^2$, 此时 $L \cong N_{2,1,2}$; 当 $in - mj \equiv 1 \pmod 2$, $i - j \equiv 0 \pmod 2$ 时, $[x, y] = b^2$, $x^2 = y^2 = b^2 c^2$, 此时 $[x, y] = (xy)^2$, 故 $L \cong M_{2,2,2}$, 当 $in - mj \equiv 1 \pmod 2$, $i - j \equiv 1 \pmod 2$ 时, $[x, y] = b^2$, $xy^{-1} = ac^{m-n}(bc)^{2i(m-n)}$, $x^2 y^2 = 1$, $[x, y] = (xy)^2$, 故 $L \cong M_{2,2,2}$, 由 x, y 的任意性,H 为 $\mathcal{T}_4$ 群. □

定理 5.1.13. *设 $p > 2$, 有限 p 群 G 为非交换的 $\mathcal{T}_4$ 群, 且 G 的所有的二元生成的非交换子群既有同构于 $M_{2,2,p}$ 的, 也有同构于 $N_{2,1,p}$ 的. 设 G 的子群 H 满足 H 的任意非交换的二元生成子群全同构于 $N_{2,1,p}$. 并且 H 的阶最大. 则可设 $H = (K \rtimes \langle b \rangle) \times E$, 其中 $K = \langle a_1 \rangle \times \langle a_2 \rangle \times \cdots \times \langle a_k \rangle \times \langle c_1 \rangle \times \langle c_2 \rangle \times \cdots \times \langle c_k \rangle \cong C_p^{2k}$, $E = \langle e_1 \rangle \times \langle e_2 \rangle \times \cdots \times \langle e_m \rangle$ 为初等交换 p 群, $a_i^b = a_i c_i, c_i^b = c_i$ 对任意的 $1 \leqslant i \leqslant k$. 则 G 同构于下列群之一:*

(1) *$H_1 \times C_p^n$, 其中 $H_1 = \langle a, b, c \mid a^p = b^{p^2} = c^{p^2} = 1, [a, b] = c^p, [a, c] = 1, [b, c] = b^p \rangle$, n 为整数;*

(2) *$H_2 \times C_p^m$, 其中 $H_2 = \langle a, b, c \mid a^p = b^{p^2} = c^{p^2} = 1, [a, b] = c^p, [a, c] = 1, [b, c] = 1 \rangle$, m 为整数;*

(3) $H_3\times C_p^m$, 其中 $H_3=\langle a,b,c \mid a^p=b^{p^2}=c^{p^2}=1,[a,b]=c^p,[a,c]=c^pb^{lp},[b,c]=1\rangle$, $1+4l$ 为模 p 平方非剩余, $(l,p)=1$, m 为整数;

(4) $H_4\times C_p^m$, 其中 $H_4=\langle a,b,c \mid a^p=b^{p^2}=c^{p^2}=1,[a,b]=c^p,[a,c]=b^{jp},[b,c]=1\rangle$, j 为固定的模 p 平方非剩余, $(j,p)=1$. m 为整数.

证明: 由题设 G 必存在子群 H 使得它的任意非交换的二元生成子群全同构于 $N_{2,1,p}$. 不妨设 H 即为满足上述条件的最大阶的子群, 由定理 5.1.10, 可设 $H=(K\rtimes\langle b\rangle)\times E$, 其中 $K=\langle a_1\rangle\times\langle a_2\rangle\times\cdots\times\langle a_k\rangle\times\langle c_1\rangle\times\langle c_2\rangle\times\cdots\times\langle c_k\rangle\cong C_p^{2k}$, E 为初等交换 p 群, $a_i^b=a_ic_i$, $c_i^b=c_i$ 对任意的 $1\leqslant i\leqslant k$.

以下证明 $\Omega_1(G)=\Omega_1(H)=K\times\langle b^p\rangle\times E$, 且 $H\trianglelefteq G$.

先证 $\Omega_1(G)=\Omega_1(H)=K\times\langle b^p\rangle\times E$, 因为 G 为 T_4 群, 由引理 5.1.1, $\Omega_1(G)$ 为交换群. 又因为 $\Omega_1(G)\trianglelefteq G$, 且 $b^p\in\Omega_1(G)$, 所以 $\Omega_1(G)\lessdot\Omega_1(G)\langle b\rangle$. 任取 $\Omega_1(G)\langle b\rangle$ 的非交换的二元生成子群 L, 我们有 $L\cap\Omega_1(G)\lessdot L$, 从而 $|\Omega_1(L)|=p^3$, 由内交换群的结构可知 $L\cong N_{2,1,p}$, 这就说明了 $\Omega_1(G)\langle b\rangle$ 的非交换子群全为 $N_{2,1,p}$. 由 H 的最大性 $|\Omega_1(G)\langle b\rangle|\leqslant|H|$, 另一方面 $\Omega_1(H)\leqslant\Omega_1(G)$, 两边同乘 $\langle b\rangle$, 即有 $|H|\leqslant|\Omega_1(G)\langle b\rangle|$. 从而有 $\Omega_1(G)=\Omega_1(H)=K\times\langle b^p\rangle\times E$, 即 H 外无 p 阶元.

再证 $H\trianglelefteq G$. 对任意的 $h\in H$, $d\in G$, 由引理 5.1.1 有 $o([h,d])\leqslant p$, 从而 $[h,d]\in\Omega_1(G)=\Omega_1(H)\leqslant H$, 即 $H\trianglelefteq G$.

此时考虑 G/H, 则 G/H 为初等交换 p 群. 设 $G/H=\langle\overline{d_1}\rangle\times\langle\overline{d_2}\rangle\times\cdots\times\langle\overline{d_l}\rangle$

以下证明 $l=1$. 若否, 由引理 5.1.11(1), (2) 有 $d_1^p=c_1^{s_{11}}b^{t_{11}p}$, $d_2^p=c_1^{s_{12}}b^{t_{12}p}$. 其中 $(s_{11},p)=1,(s_{12},p)=1$. 从而必存在 u,v 使得 $(v,p)=1,(u,p)=1$. 且 $c_1=d_1^{up}b^{-ut_{11}p}=d_2^{vp}b^{-vt_{12}p}$. 此时 $(d_1^ub^{-ut_{11}}d_2^{-v}b^{vt_{12}})^p=1$, H 外有 p 阶元与 $\Omega_1(G)=\Omega_1(H)$ 矛盾.

从而令 $H=(K\rtimes\langle b\rangle)\times E=(\langle a\rangle\rtimes\langle b\rangle)\times E$, $G/H=\langle\bar{d}\rangle$, 从而 $G=H\langle d\rangle$.

从而不妨设 $d^p=c=[a,b]$, 若否, 由前面有 $c=d^{up}b^{-utp}$, 用 d^ub^{-ut} 代替 d 即可. 因为 $\langle d^p\rangle\neq\langle b^p\rangle$, 由题设 G 子群结构可设 $[b,d]=b^{ip}d^{jp}$, 其中 i,j 为整数. 同理 $[ba,d]=b^{sp}d^{tp}$, 其中 s,t 为整数. 从而 $[a,d]=b^{(s-i)p}d^{(t-j)p}\in\langle b^p,d^p\rangle$. 以下分情况讨论:

情况一. $[a,d]=1$,

不妨设 $[b,d]=b^{ip}$, 若否, 由 $[b,d]=b^{ip}d^{jp}$, 可用 da^j 代替 d, 以下分情况讨论:

当 $(i,p)=1$ 时, 用 $a^{i^{-1}},d^{i^{-1}}$ 代替 a,d, 可得出 $[b.d]=b^p$, 得出群 H_1.

当 $(i,p)\neq 1$ 时, 即 $i|p$, 则 $[b,d]=1$, 得出群 H_2.

情况二. $[a,d]\neq 1$,

不妨设 $[b,d]=1$,

若否, 由前面分析可知总存在 u,v 使得 $[b,d]=d^{up}[a,d]^v$, 从而 $\langle b^p,d^p\rangle=\langle d^p,[a,b]\rangle$, 又因为 $[ba^{-v},da^u]=[b,d]d^{-u}[a,d]^{-v}=1$, 用 ba^{-v},da^u 分别代替 b,d 即可. 由 $[a,d]\in\langle b^p,d^p\rangle$, 可设 $[a,d]=d^{ip}b^{jp}$, 其中 $(j,p)=1$(若否 $\langle a,d\rangle$ 为 p^3 阶群, 与题设矛盾.)

考虑 $\langle a,db^x\rangle$,$[a,db^x]=d^{(i+x)p}b^{jp}$, 又

$\langle a,db^x\rangle$ 为非交换 T_4 群 $\Rightarrow \begin{vmatrix} 1 & x \\ i+x & j \end{vmatrix}\equiv 0$ 无解

$\Rightarrow x^2+ix-j\equiv 0$ 无解. 即 i^2+4j 为平方剩余. 从而不妨设 $[a,d]=d^pb^{jp}$ 或 $[a,d]=b^{jp}$. (若 $[a,d]\neq b^{jp}$ 可用 $a^{i^{-1}},b^i$ 代替 a,b, 即得出 $[a,d]=d^pb^{lp}$, 其中 $(l,p)=1$.)

当 $[a,d]=d^pb^{lp}$ 时, G 为 T_4 群 $\Leftrightarrow 1+4l$ 为模 p 平方非剩余. 此时的出群 H_3.

当 $[a,d]=b^{jp}$ 时, G 为 T_4 群 $\Leftrightarrow j$ 为模 p 平方非剩余. 此时的出群 H_4.

查看 p^5 阶 $\mathcal{A}_2$ 群表可知定理中 H_1, H_2, H_3, H_4 为 p^5 阶 $\mathcal{A}_2$ 群表中互不同构的群.

要证明 G 为 T_4 群, 由定理 5.1.1(7) 可知, 只需证明 H_1, H_2, H_3, H_4 为 T_4 群即可. 又由 $\mathcal{A}_2$ 群定义可知 H_1, H_2, H_3, H_4 为 T_4 群. □

§5.2 小结

本节将上节的主要结果重述并挑出其中的亚 Hamilton 群.

定理 5.2.1. 设 G 为非交换的 T_4 群, 若 G 有子群同构于 $M_{3,1,p}$, 则 $G\cong M_{3,1,p}\times C_p^n$.

定理 5.2.2. 设 G 为非交换的 T_4 群, 且 G 的所有的非交换二元生成子群均同构于 $N_{2,1,p}$. 则 $G \cong H \times C_p^n$. 其中 $H = K \rtimes \langle a \rangle$ 是 $K = \langle b_1 \rangle \times \langle b_2 \rangle \times \cdots \times \langle b_k \rangle \times \langle c_1 \rangle \times \langle c_2 \rangle \times \cdots \times \langle c_k \rangle \cong C_p^{2k}$ 被 $\langle a \rangle$ 的循环扩张, 满足 $a^{p^2} = 1$, 且 $b_i^a = b_i c_i, c_i^a = c_i$ 对任意的 $1 \leqslant i \leqslant k$ 成立.

定理 5.2.3. 设 G 为非交换的 T_4 群, 且 G 的所有的非交换二元生成子群均同构于 $M_{2,2,p}$. 其中 $p > 2$. 则 $G \cong H \times C_p^n$. 其中 $H = K \rtimes \langle b \rangle$ 是 $K = \langle a_1 \rangle \times \langle a_2 \rangle \times \ldots \langle a_k \rangle \cong C_{p^2}^k$ 被 p^2 阶群 $\langle b \rangle$ 的循环扩张. 满足 $a_i^b = a_i^{1+p}$ 对任意的 $1 \leqslant i \leqslant k$ 成立.

定理 5.2.4. G 为非交换的 T_4 群, 若 G 的所有的二元生成的非交换子群均同构于 $M_{2,2,2}$, 则 G 为以下群之一:

(1) $H \times C_2^n$. 其中 $H = K \rtimes \langle b \rangle$ 是 $K = \langle a_1 \rangle \times \langle a_2 \rangle \times \ldots \langle a_k \rangle \cong C_4^k$ 被 $\langle b \rangle$ 的循环扩张, 满足 $b^4 = 1$ 且 $a_i^b = a_i^{-1}$ 对任意的 $1 \leqslant i \leq k$ 成立;

(2) $H \times C_2^n$. 其中 $H = \langle a_1, a_2, b \mid a_1^4 = a_2^4 = 1, b^2 = a_1^2, [a_1, a_2] = 1, [a_1, b] = a_2^2, [a_2, b] = a_1^2 \rangle$;

(3) $H \times C_2^n$. 其中 $H = \langle a_1, a_2, b, d \mid a_1^4 = a_2^4 = 1, b^2 = a_1^2, d^2 = a_2^2, [a_1, a_2] = 1, [a_1, b] = a_2^2, [a_2, b] = a_1^2, [a_1, d] = a_1^2, [a_2, d] = a_1^2 a_2^2, [b, d] = 1 \rangle$.

定理 5.2.5. 设 G 为非交换的 T_4 群, 且 G 的非交换的二元生成子群既有同构于 $N_{2,1,p}$ 的, 也有同构于 $M_{2,2,p}$ 的. 则 $G \cong L \times C_p^n$. 其中 L 为以下 p^5 阶的 $\mathcal{A}_2$ 群之一:

(1) $\langle a, b \rangle * C_{p^2}$. 其中 $\langle a, b \rangle \cong N_{2,1,p}$. 即 $G = \langle a, b, d \mid a^{p^2} = b^p = d^{p^2} = 1, [a, b] = d^p, [d, a] = [d, b] = 1 \rangle$;

(2) $\langle a, b \rangle \rtimes C_p$. 其中 $\langle a, b \rangle \cong M_{2,2,p}$ 且 $p > 2$. 即 $G = \langle a, b, d \mid a^{p^2} = b^{p^2} = d^p = 1, [a, b] = a^p, [d, a] = b^p, [d, b] = 1 \rangle$;

(3) $\langle a, b, d \mid a^p = b^{p^2} = d^{p^2} = 1, [a, b] = d^p, [d, a] = b^{-\nu p}, [d, b] = 1 \rangle$, $p > 2$ 且 ν 是一个固定的模 p 的平方非剩余;

(4) $\langle a, b, d \mid a^p = b^{p^2} = d^{p^2} = 1, [a, b] = d^p, [d, a] = b^{jp}d^p, [d, b] = 1\rangle$, 若 p 为奇数, 则 $4j = 1 - \rho^{2r+1}$, $1 \leqslant \rho \leqslant \frac{p-1}{2}$, ρ 是模 p 的简化剩余系的一个原根; 若 $p = 2$, 则 $j = 1$.

定理 5.2.6. 设 G 是有限亚 *Hamilton* p 群, $|G'| \geqslant p^2$. 若 G 又是 T_4 群, 则 G 只可能是定理 5.2.4 中的 (2), (3) 型群或者定理 5.2.5 中的 (2), (3), (4) 型群.

证明 首先, 若 G 是定理 5.2.1 中的群或者定理 5.2.5 中的 (1) 型群, 则 $|G'| = p$, 不符合题设条件. 我们只需要证明其它的 $|G'| \geqslant p^2$ 的群都不是有限亚 Hamilton p 群.

若定理 5.2.2 中的群 $|G'| \geqslant p^2$, 则有 $k \geqslant 2$. 因为 $\langle b_1, a\rangle$ 既不交换也不正规, 所以 G 不是有限亚 Hamilton p 群.

若定理 5.2.4 中的群 $|G'| \geqslant p^2$, 则有 $k \geqslant 2$. 因为 $\langle a_1, b\rangle$ 既不交换也不正规, 所以 G 也不是有限亚 Hamilton p 群. □

第六章　有限亚 Hamilton 群

我们知道, 单群即没有非平凡的正规子群的群. 与之相对应的概念是 Dedikind 群, 即所有子群都正规的群. 对于 Dedikind 群的研究始于十九世纪末. 1897 年, R. Dedekind 对于有限 Dedikind 群进行了分类, 见 [21]. 随后, 1933 年, R. Baer 分类了无限 Dedikind 群, 见 [15]. 众所周知, Hamilton 群就是非交换的 Dedikind 群, 即每个子群均正规的非交换群. 下面的定理给出了有限 Hamilton 群的结构:

定理 6.0.7. *设 Q_8 是四元数群, A 是奇阶交换群, B 是初等交换 2 群. 则 $Q_8 \times A \times B$ 是 Hamilton 群. 反过来, 每个有限 Hamilton 群都有上述之形状.*

定义 6.0.8. *设 G 是非交换群, 称 G 为 亚 Hamilton 群, 如果 G 的每个非交换子群都正规.*

亚 Hamilton 群是 Hamilton 群的一个很自然的推广. 二十世纪六、七十年代, V. T. Nagrebeckii[46, 47, 48] 以及 G. M. Romalis 和 N. F. Sesekin[55, 56, 57] 对于亚 Hamilton 群已经做了大量的工作. 其中 G. M. Romalis 和 N. F. Sesekin 主要考虑的是无限亚 Hamilton 群的一些性质. 而 V. T. Nagrebeckii 则主要考虑有限亚 Hamilton 群. V. T. Nagrebeckii 在 [47] 中证明了下面的定理.

定理 6.0.9. *设 G 是有限非幂零群, 则 G 是亚 Hamilton 群当且仅当 $G = SZ(G)$, 其中 S 是下列群之一:*

(1) $S = P \rtimes Q$, 其中 P 是初等交换 p 群, Q 循环并且 $(p, |Q|) = 1$;

(2) $S = P \rtimes Q$, 其中 $P \cong Q_8$ 且 Q 是奇阶循环群;

(3) $S = P \rtimes Q$, 其中 $|P| = p^3, p \geqslant 5$, Q 循环并且 $(p, |Q|) = 1$.

根据这个定理, 我们考虑亚 Hamilton 群, 仅需考虑幂零的情形. 又注意到幂零群是其诸 Sylow 子群的直积, 因此其实只需考虑亚 Hamilton p 群. 而它们的结构远比非幂零的情况复杂.

二十世纪八十年代, N. F. Kuzennyi 和 N. N. Semko 一些特殊的亚 Hamilton p 群进行了分类. 但是, 他们主要关注的是无限群的情形. 另外, 他们的文章不易

找到. 从目前我们找到文献 [44] 和 [45] 来看, 他们没有解决同构问题, 有些群的结果甚至只能看作群 G 为亚 Hamilton p 群的必要条件.

值得提出的是, 国内的学者也研究过有限亚 Hamilton p 群. 吕恒、陈贵云在 [2] 中证明了对于 $p \neq 2$、5, 有限亚 Hamilton p 群的幂零类至多为 4. 但他们没有找到幂零类为 4 的亚 Hamilton p 群的例子. 在本书中我们进一步证明了亚 Hamilton p 群的幂零类不超过 3. 从而我们知道亚 Hamilton p 群一定是亚交换 p 群.

本章我们给出了有限亚 Hamilton p 群的一些基本性质. 在下一章完成了有限亚 Hamilton p 群的完全分类, 并彻底解决了同构问题. 从而最终解决了有限亚 Hamilton 群的分类问题.

§6.1 有限亚 Hamilton p 群的基本性质

定理 6.1.1. *设 G 是有限群 p 群, 则 G 是亚 Hamilton 群当且仅当它的每个二元生成的非交换子群都正规.*

定理 6.1.2. *有限亚 Hamilton p 群 G 的幂零类至多为 3. 特别地 G 为亚交换群.*

定理 6.1.3. *设 G 是有限 p 群, 则 G 是亚 Hamilton 群当且仅当 G 的导群包含在它的每个非交换子群之中.*

上面的定理是有限亚 Hamilton p 群的基本性质, 也是本节的主要结论. 我们首先做一些简单的准备, 然后再给出定理的证明.

引理 6.1.4. *设 G 是有限亚 Hamilton 群, 则 G 的每个截断都是亚 Hamilton 群.*

证明 直接验证即可. □

引理 6.1.5. *设 G 是有限非交换 p 群, 则 G 的交换极大子群的个数是 1 或 $1+p$.*

证明　设 G 有两个不同的交换极大子群 A_1 和 A_2, 则 $A_1 \cap A_2$ 为 G 的指数为 p^2 的子群, 并且 $A_1 \cap A_2 \leqslant Z(G)$. 因为 G 非交换, 所以 $Z(G) = A_1 \cap A_2$. 因为 G 的每个交换极大子群都包含 $Z(G)$, 所以其个数与 $G/Z(G)$ 的 p 阶子群的个数相同, 为 $1+p$ 个. □

引理 6.1.6. *设 G 是有限亚 Hamilton p 群, $x \in G$. 则 x 的正规闭包 $\langle x \rangle^G$ 是交换群或者内交换群.*

证明　若 $\langle x \rangle^G$ 不交换, 则存在 $g \in G$ 使得 $[x, x^g] \neq 1$. 由定义, $K := \langle x, x^g \rangle \trianglelefteq G$. 于是 $K = \langle x \rangle^G$. 令 $y = x^g$. 因为 $\langle x, x^y \rangle$ 是 K 的真子群, 若 $[x, x^y] \neq 1$, 则亦有 $\langle x, x^y \rangle = \langle x \rangle^G = K$, 矛盾. 因此, 我们有 $[x, x^y] = 1$. 由此得 $[x, y, x] = 1$. 交换 x 和 y 的位置, 又可得 $[x, y, y] = 1$. 于是 $c(K) = 2$.

再考虑 K 的真子群 $\langle x, y^p \rangle$. 同样的道理可得 $[x, y^p] = 1$. 因 $c(K) = 2$, 有 $[x, y]^p = 1$. 这推出 $K' = \langle [x, y] \rangle$ 是 p 阶群. 由定理 2.1.4 得 K 内交换. □

下面我们给出本节主要结论的证明.

定理 6.1.1 的证明: 必要性显然. 我们只需证明充分性:

用反证法. 假设 G 不是亚 Hamilton 群, 则 G 中存在不正规的非交换子群. 设 H 是阶最小的一个 G 的不正规的非交换子群. 由题设 H 不是二元生成的, 从而 H 至少有 $1+p+p^2$ 个极大子群. 再由引理 6.1.5 可知, H 至少有两个非交换的极大子群 N_1 和 N_2. 由 H 的极小性, N_1 和 N_2 都是 G 的正规子群. 从而 $H = N_1 N_2$ 也是 G 的正规子群, 矛盾. □

定理 6.1.2 的证明: 由引理 6.1.6, 任何元素 x 的正规闭包 $K = \langle x^g \rangle$ 若不交换, 则内交换. 在 K 内交换的情况下, K' 作为 K 的特征子群, 是 G 的阶为 p 的正规子群. 于是 $K' \leqslant Z(G)$. 这样, $G/Z(G)$ 中任何元素之正规闭包均交换, 从而 $G/Z(G)$ 满足 2-Engel 条件. 由定理 1.2.2, 只要 $p \neq 3$, 就有 $c(G) \leqslant 3$; 而若 $p = 3$, 有 $c(G) \leqslant 4$.

现在假定 $p = 3$, 我们也来证明 $c(G) \leqslant 3$. 设 G 是极小阶反例, 则由引理 6.1.4 可知 $c(G) = 4$, $|G_4| = p$, 并且 G 的每个真子群和真商群的幂零类至多为 3. 于是可设 $G_4 = \langle [a, b, c, d] \rangle$, $a, b, c, d \in G$. 还不妨设 $a, b, c, d \notin \Phi(G)$. 记 $x = [a, b, c]$, 则 $N = \langle x, d \rangle$ 为内交换群. 从而 $N \trianglelefteq G$, 并由定理条件, 包含 N 的

子群皆在 G 中正规. 这得到 G/N 为 Dedekind 群. 因为 $p=3$, G/N 交换. 又由 $d \notin \Phi(G)$ 知 $G' \leqslant N \cap \Phi(G) < N$, 从而 G' 交换. 于是 $[[c,d],[a,b]]=1$. 又由 $[a,b] \in N$ 和 $d \in N$, 知 $[d,[a,b]] \in N' \leqslant Z(G)$, 从而 $[d,[a,b],c]=1$. 最后应用命题 1.1.2(4) 可得 $[[a,b],c,d]=1$, 矛盾. □

定理 6.1.3 的证明: 充分性显然, 下面证明必要性.

设 G 是极小阶的反例. 则 G 中存在内交换的子群 $N=\langle a,b\rangle$ 使得 $G' \not\leqslant N$. 由于 G 为亚 Hamilton 群, G 的包含 N 的子群全都正规, 从而 G/N 为 Hamilton 群. 由 G 的极小性, $G/N \cong Q_8$. 令 $G/N=\langle xN, yN\rangle$, $H=\langle x,y\rangle$. 则 $G=HN$, $H/(H\cap N)\cong Q_8$, $z:=[x,y] \notin N$, $H\cap N \leqslant \Phi(H)$ 且 $H \cap N = \langle x^4, x^2y^2, x^2[x,y]\rangle^H$. 易知 $z \in \langle x\rangle^H$. 由引理 6.1.6 可知, $\langle z,x\rangle$ 交换或内交换, 从而一定有 $[z,x]^2=[z,x]^2=1$. 同理 $[z,y^2]=[z,y]^2=1$. 这首先说明 $\exp(H_3)\leqslant 2$. 又因为 $\Phi(H)=\langle x^2,y^2,H'\rangle$, 以及 H' 交换 (定理 6.1.2), 可得 $[\Phi(H),z]=1$. 特别地, $[H\cap N,z]=1$. 下面我们分五种情形推出矛盾:

(1) $H\cap N=N$:

此时 $[N,z]=1$. 设 $M=\langle za,b\rangle$, 则由定理 2.1.4 可知 M 为内交换群, 从而 G/M 也是 Hamilton 群. 由于 $z\notin M$, G/M 非交换. 再由 G 的极小性可知 $H/M=G/M\cong Q_8$. 所以又有 $M=\langle x^4, x^2y^2, x^2[x,y]\rangle^H=N=\langle a,b\rangle$, 矛盾.

(2) $H\cap N<N$ 且 $H\cap N \not\leqslant \Phi(N)$:

此时, $H\cap N$ 包含 N 的一个生成元. 不妨设 N 的生成元 $a\in H\cap N$, $b\notin H\cap N$. 则 $[z,a]=1$. 因为 $H\cap N$ 交换, 所以 $[x^2y^2, x^2[x,y]]=1$, 进而 $[x^2,y^2]=1$. 通过计算, $[x^2,y^2]=[x^2,y]^2=[x,y]^4=z^4$. 若 $z^2\neq 1$, 则有 $\langle z^2\rangle=\mho_1(H')$ 为 G 的极小正规子群. 所以总有 $z^2\in Z(G)$. 特别地, $[z,b]^2=[z^2,b]=1$.

(i) 若 $[z,b]\neq[a,b]$. 令 $M=\langle za,b\rangle$, 由定理 2.1.4 可知 M 为内交换群, 从而 G/M 也是 Hamilton 群. 由于 $z\notin M$, G/M 非交换. 再由 G 的极小性可知 $G/M=HM\cong H/(H\cap M)\cong Q_8$. 所以又有 $H\cap M=\langle x^4, x^2y^2, x^2[x,y]\rangle^H = H\cap N$, 从而 $a\in H\cap N=H\cap M\leqslant M$. 进一步有 $z=(za)a^{-1}\in M$, 矛盾.

(ii) 若 $[z,b]=[a,b]$. 则 $L:=\langle z,b\rangle\cap N$ 为 G 的包含 b 的正规子群. 令 K 为 N 的包含 L 的极大子群, 且 $K\trianglelefteq G$, 则 G/K 一定是二元生成的 2^4 阶群, 且它有商群与 Q_8 同构. 由 2^4 阶群的分类可知, $G/K=\langle xK, yK\rangle:=\langle\bar{x},\bar{y}\rangle\cong M_2(2,2)$.

其定义关系为:

$$\bar{x}^4 = \bar{y}^4 = 1, [\bar{x}, \bar{y}] = \bar{x}^2$$

易知, $\langle\bar{y}\rangle$ 和 $\langle\bar{x}\bar{y}\rangle$ 均为 G/K 的不正规的子群, 所以, 它们的完全反像也是 G 的不正规的子群, 从而是交换群. 由此我们有 $[y, K] = 1$, $[xy, K] = 1$, 进而 $[H, K] = 1$. 这与 $[z, b] = [a, b] \neq 1$ 矛盾.

(3) $H \cap N < \Phi(N)$:

此时, 首先我们断言 $H \cap N \neq 1$: 若否, 则 $G = H \times N$. 因为 $N \cong G/H$ 一定是 Hamilton 群, 所以 $N \cong Q_8$. 此时 $\langle xa, yb\rangle \cong Q_8$ 在 G 中不正规, 矛盾.

我们还可以进一步断言 $N' \leqslant H \cap N$: 若否, 则 $G/(H \cap N)$ 也是反例, 与 G 的极小性矛盾.

令 $\overline{G} = G/(H \cap N)$, $\overline{H} = H/(H \cap N) = \langle\bar{x}, \bar{y}\rangle$, $\overline{N} = N/(H \cap N) = \langle\bar{a}\rangle \times \langle\bar{b}\rangle$, 则 $\overline{G} = \overline{H} \times \overline{N}$. 且 $\overline{N}$ 中必有阶不小于 4 的元素, 不妨设 $o(\bar{a}) \geqslant 4$. 设 $\overline{K} = \langle\bar{x}\bar{a}\rangle \times \langle\bar{b}\rangle$, 则 $\overline{K}$ 在 $\overline{G}$ 中不正规, 所以它的完全反像在 G 中也都不正规, 从而是交换群. 这意味着 $[xa, b] = 1$(即 $[x, b] = [a, b]$). 将 $\bar{x}$ 换为 $\bar{y}$ 或 $\bar{x}\bar{y}$ 后, 同理可得 $[y, b] = [a, b]$ 和 $[xy, b] = [a, b]$. 而这是不可能的.

(4) $H \cap N = \Phi(N) = N'$:

此时, $|N| = 2^3$, $|H| = 2^4$, $|G| = 2^6$, 且 $G/N' = H/N' \times \langle aN'\rangle \times \langle bN'\rangle$. 因为 $\langle aN'\rangle$ 和 $\langle bN'\rangle$ 在 G/N' 中正规, 所以它们的完全反像 $A := \langle a, N'\rangle$ 和 $B := \langle b, N'\rangle$ 在 G 中也正规. 注意到 A 和 B 均为 4 阶群. 由 NC 定理可知, $C_G(A)$ 和 $C_G(B)$ 均为 G 的极大子群. 令 $K = C_G(A) \cap C_G(B)$, 则 $|K| \geqslant 2^4$. 因为 $K \cap N = Z(N) = N'$, 所以 $|KN| = (|K||N|)/|K \cap N| \geqslant 2^6$. 从而 $G = K * N$. 因为 $KN/N \cong K/K \cap N \cong Q_8$. 我们不妨设 $H = K$. 由 2^4 阶群的分类可知, $H = \langle x, y\rangle \cong M_2(2, 2)$. 其定义关系为:

$$x^4 = y^4 = 1, [x, y] = x^2$$

且 $N' = H \cap N = \langle x^2y^2\rangle$. 设 a 为 N 中的 4 阶元, 则 $a^2 = x^2y^2$. 计算可知 $[x, ay] = x^2$, $(ay)^2 = x^2$. 从而子群 $\langle x, ay\rangle$ 既不交换也不正规, 矛盾.

(5) $H \cap N = \Phi(N) \neq N'$

令 K 为 $H \cap N$ 的极大子群, 且在 G 中正规. 我们首先断言 $N' \leqslant K$: 若否, 则 G/K 也是反例, 与 G 的极小性矛盾. 所以断言成立. 从而 N/K 为交换群. 设

$\overline{G}=G/K$, $\overline{H}=H/K=\langle\bar{x},\bar{y}\rangle$, $\overline{N}=N/K=\langle\bar{a}\rangle\times\langle\bar{b}\rangle$. 其中 $o(\bar{a})=4$. 由 2^4 阶群的分类可知, $H/K\cong M_2(2,2)$. 其定义关系为:

$$\bar{x}^4=\bar{y}^4=1,[\bar{x},\bar{y}]=\bar{x}^2$$

且 $\bar{a}^2=\bar{x}^2\bar{y}^2$, $\Phi(N)/K=(H\cap N)/K=\langle\bar{x}^2\bar{y}^2\rangle$. 我们有 $\bar{a}\notin Z(\overline{G})$ (若否, 则 $\langle\bar{x},\bar{a}\bar{y}\rangle$ 在 $\overline{G}$ 中既不交换也不正规, 矛盾). 我们还有 $[\bar{a},\bar{x}]\neq 1$(若否, 由 $\bar{a}\notin Z(\overline{G})$ 可得 $[\bar{a},\bar{y}]=\bar{x}^2\bar{y}^2$, 从而 $\langle\bar{a}\bar{x},\bar{y}\rangle$ 在 $\overline{G}$ 中既不交换也不正规, 矛盾). 所以必有 $[\bar{a},\bar{x}]=\bar{x}^2\bar{y}^2$. 将上面的 a 换为 $\bar{a}\bar{b}$ 考虑, 同理可得 $[\bar{a}\bar{b},\bar{x}]=\bar{x}^2\bar{y}^2$, 从而 $[\bar{b},\bar{x}]=1$. 我们又有 $[\bar{b},\bar{y}]=\bar{1}$(若否, 则 $[\bar{b},\bar{y}]=\bar{x}^2\bar{y}^2$. 计算可知 $\langle\bar{x},\bar{b}\bar{y}\rangle$ 在 $\overline{G}$ 中既不交换也不正规, 矛盾).

现在, 容易看出 $\langle\bar{x},\bar{b}\rangle$ 和 $\langle\bar{a}\bar{x},\bar{b}\rangle$ 在 $\overline{G}$ 中均不正规, 所以它们的完全反像在 G 中也不正规, 从而交换. 所以我们有 $[x,b]=1$ 以及 $[ax,b]=1$. 这与 $[a,b]\neq 1$ 矛盾. □

§6.2 有限亚 Hamilton p 群的性质

定理 6.2.1. 设 G 是导群初等交换的有限亚 *Hamilton* p 群, 且 $c(G)=3$, 则 G 一定是 $\mathcal{A}_2$ 群.

上面的定理是本节的主要结论. 我们先证明两个引理:

引理 6.2.2. 设 G 是导群初等交换的有限亚 *Hamilton* p 群. 若 G 不是 $\mathcal{A}_2$ 群, 则 G 的 $\mathcal{A}_2$ 子群都是类 2 的.

证明 假设结论不成立, 则 G 中存在导群初等交换的类 3 的 $\mathcal{A}_2$ 子群 K. 由推论 4.6.2 可知, p 为奇素数且 K 只能是以下几种群之一:

(1) p^4 阶的极大类 p 群:

(i) $\langle a,b,c,d \mid a^p=b^p=c^p=d^p=1,[c,d]=b,[b,d]=a,[a,b]=[a,c]=[a,d]=[b,c]=1\rangle$;

(ii) $\langle a,b,c \mid a^{p^2}=b^p=1,c^p=a^{\alpha p},[a,b]=a^p,[a,c]=b,[b,c]=1\rangle$, 其中 $\alpha=0,1$ 或是一个模 p 的平方非剩余 (三种互不同构的群);

(iii) $p=3$, $\langle a,b,c \mid a^9=b^3=c^3=1,[a,b]=1,[a,c]=b,[c,b^{-1}]=a^{-3}\rangle$.

(2) 二元生成有交换极大子群的 $\mathcal{A}_2$ 群 $(n\geqslant 5)$:

(i) $\langle b,a_1,a_2,a_3 \mid b^{p^{n-3}}=a_1^p=a_2^p=a_3^p=1,[a_1,b]=a_2,[a_2,b]=a_3,[a_i,a_j]=1,[a_3,b]=1\rangle$, 其中 $1\leqslant i,j\leqslant 3$;

(ii) $\langle b,a_1,a_2 \mid b^{p^{n-2}}=a_1^p=a_2^p=1,[a_1,b]=a_2,[a_2,b]=b^{p^{n-3}},[a_1,a_2]=1,[b^{p^{n-3}},a_1]=[b^{p^{n-3}},a_2]=1\rangle$;

(iii) $\langle b,a_1,a_2 \mid b^{p^{n-3}}=a_1^{p^2}=a_2^p=1,[a_1,b]=a_2,[a_2,b]=a_1^{\nu p},[a_1,a_2]=1,[a_1^p,b]=[a_1^p,a_2]=1\rangle$, 其中 $\nu=1$ 或者 ν 是一个固定的模 p 的平方非剩余.

(3) 无交换极大子群的 $\mathcal{A}_2$ 群 $(p\geqslant 5)$:

(i) $\langle a,b \mid a^{p^2}=b^{p^2}=c^p=1,[a,b]=c,[c,a]=b^{\nu p},[c,b]=a^p\rangle$, 其中 ν 是固定的模 p 的平方非剩余;

(ii) $\langle a,b \mid a^{p^2}=b^{p^2}=c^p=1,[a,b]=c,[c,a]=a^{-p}b^{-lp},[c,b]=a^{-p}\rangle$, 其中 $4l=g^{2r+1}-1$ 对于 $r=1,2,\ldots,\frac{1}{2}(p-1)$, g 是模 p 的最小原根;

(4) 无交换极大子群的 $\mathcal{A}_2$ 群 $(p=3)$:

(i) $\langle a,b \mid a^9=b^9=c^3=1,[a,b]=c,[c,a]=b^{-3},[c,b]=a^3\rangle$;

(ii) $\langle a,b \mid a^9=b^9=c^3=1,[a,b]=c,[c,a]=b^{-3},[c,b]=a^{-3}\rangle$.

我们设 H 是 G 的一个以 K 为极大子群的子群, 然后分情况推出矛盾.

情形 1: K 为上面所列的 (2) 型群.

易知 $K/Z(K)$ 为 p^3 阶的非亚循环的内交换群. 则 $H/Z(K)$ 为非亚循环的 p^4 阶群. 若 $d(H/Z(K))=2$, 由 p^4 阶群的分类可知 $H/Z(K)$ 是极大类的. 从而 $K'Z(K)/Z(K)=H_3Z(K)/Z(K)$. 这说明 $[a_1,b]\in H_3Z(K)$, 从而 $[a_1,b,b]\in H_4$. 由于 $[a_1,b,b]\neq 1$, $H_4\neq 1$, 从而 $c(H)\geqslant 4$. 这与定理 6.1.2 矛盾. 若 $d(H/Z(K))=3$, 由 p^4 阶群的分类可知存在 $d\in H$ 使得 $H/Z(K)=K/Z(K)\times\langle dZ(K)\rangle$ 或者 $H/Z(K)=K/Z(K)*\langle dZ(K)\rangle$. 取 $k\in K$, 由命题 1.1.3 计算可得 $[d^p,k]=[d,k]^p$. 因为 $\exp(G')=p$, 所以对于 $k\in K$ 有 $[d^p,k]=1$. 从而 $d^p\in Z(K)$, 只有 $H/Z(K)=K/Z(K)\times\langle dZ(K)\rangle$. 则我们

有 $d^p \in Z(K)$, $[K,d] \in Z(K)$. 由于 $a_2 = [a_1, b] \notin \langle a_1, d\rangle$, 由定理 6.1.3 可知 $[a_1, d] = 1$. 同理可知 $[b, d] = 1$, 从而 $d \in Z(H)$. 此时 $\langle a_2 d, b\rangle$ 既不交换也不正规, 矛盾.

情形 2: K 为上面所列的 (1) 型群.

这种情况与情形 1 是类似的. 事实上, 只要在 (2) 型群中让 $n = 4$, 就会得到 (1) 中的 (i), (ii) 型群.

情形 3: K 为上面所列的 (3) 型群或 (4) 型群.

由定理 6.1.3, $H' \leqslant \langle c, a\rangle \cap \langle c, b\rangle = \langle c, a^p, b^p\rangle$. 从而 $H' = K'$, $H_3 = K_3 = \langle a^p, b^p\rangle$. 因为 H/K_3 为导群 p 阶的 p^4 阶群, 由 p^4 阶群的分类易知存在 $d \in H\backslash K$ 使得 $[a, d] \equiv [b, d] \equiv 1 (\mathrm{mod}\ K_3)$. 由于 $\exp(H') = p$, 利用命题 1.1.3 计算可得, $[a, d^p] = [a, d]^p = 1$ 且 $[b, d^p] = [b, d]^p = 1$. 从而 $d^p \in Z(K) = K_3$. 因为 $c \notin \langle a, d\rangle$, 由定理 6.1.3 可知 $[a, d] = 1$. 同理可知 $[ac, d] = 1$. 此时子群 $\langle a, cd\rangle$ 既不交换也不正规, 矛盾. □

引理 6.2.3. *设 G 是导群初等交换的有限亚 Hamilton p 群. 若 G 的 $\mathcal{A}_2$ 子群都是类 2 的, 则 G 的幂零类也是 2.*

证明 设 G 为极小阶反例. 则 $c(G) = 3$.

首先我们证明 G 不满足 2-engle 条件. 若否, 则由定理 1.2.2 可知 G 是 3-群. 此时, 存在 $x, y, z \in G$, 使得 $[x, y, z] \neq 1$. 由于 G 为极小阶反例, 我们有 $G = \langle x, y, z\rangle$, 且 $[x, y, z]^3 = [x^3, y, z] = 1$. 由 $[x, yz, yz] = 1$ 可得, $[x, y, z] = [z, x, y]$. 同理可知, $[x, y, z] = [y, z, x] = [z, x, y]$. 设 $[x, y] = c$, $[y, z] = a$, $[z, x] = b$, $[x, y, z] = [y, z, x] = [z, x, y] = d$, 则 $G' = \langle a, b, c, d\rangle$. 因为 $[b, y] = d \neq 1$, 所以 $\langle b, y\rangle$ 不交换, 从而 $\langle b, y\rangle \trianglelefteq G$. 所以我们有 $c = [x, y] \in \langle b, y\rangle$. 注意到 $[c, b] = [c, y] = 1$, 我们可设 $c = y^{3t} d^w$. 从而 $d = [c, z] = [y^{3t} d^w, z] = [y^{3t}, z] = 1$, 矛盾.

由于 G 不满足 2-engle 条件, 存在 $[x, y, y] \neq 1$. 由 G 为极小阶反例可知 $G = \langle x, y\rangle$, 且 $[x, y, y]^p = 1$, $[x, y, x]^p = 1$. 令 $[x, y] = c$, $[c, y] = b$, $[c, x] = a$, 则 $G_3 = \langle b, a\rangle$, $G' = \langle c, G_3\rangle$. 若 $[c, x] \in \langle b\rangle$, 经过替换我们可不妨设 $[c, x] = a = 1$. 所以我们总有 $\langle a\rangle \cap \langle b\rangle = 1$.

G 有 $p+1$ 个极大子群, 分别是 $M = \langle x^i y, \Phi(G)\rangle$ 和 $K = \langle x, \Phi(G)\rangle$, 其中 $i = 0, 1, \ldots, p$, $\Phi(G) = \langle x^p, y^p, c, a, b\rangle$. 易知 $\Phi(G)$ 是交换群.

因为 $[x,x^iy]=[x,y]=c$, $[c,x^iy]=a^ib\neq 1$, 所以 $N=\langle c,x^iy\rangle$ 是 x^iy 在 G 中的正规闭包, 并且 N 是内交换群. 由定理 6.1.3, $G'\leqslant N$. 由于 $[cx^p,x^iy]=ba^{i+iC_p^2}\neq 1$, $\langle cx^p,x^iy\rangle$ 也是内交换群, 从而 $\langle cx^p,x^iy\rangle=N$, 这使得 $x^p\in N$. 由于 $(x^iy)^p\equiv x^{ip}y^p \pmod{G'}$, $x^{ip}y^p\in N$, 进而 $y^p\in N$. 这说明 $\Phi(G)\leqslant N$, 从而 $M=N$ 是内交换群.

若 $[c,x]=a\neq 1$, 我们令 $L=\langle c,x\rangle$. 此时 L 是 x 在 G 中的正规闭包, 并且 L 是内交换群. 由定理 6.1.3, $G'\leqslant L$. 由于 $[cy^p,x]=\neq 1$, $\langle cy^p,x\rangle$ 也是内交换群, 从而 $\langle cy^p,x\rangle=L$, 这使得 $y^p\in L$. 这说明 $\Phi(G)\leqslant L$, 从而 $K=L$ 是内交换群.

若 $[c,x]=a=1$ 且 p 为奇素数, 则 $[x,y^p]=1$. 从而 $[\Phi(G),x]=1$. 此时 K 为交换群;

若 $[c,x]=a=1$ 且 $p=2$, 则 $[x,y^2]=b\neq 1$. 所以 $L=\langle x,y^2\rangle\trianglelefteq G$, 并且 L 为交换群. 由定理 6.1.3, $G'\leqslant L$. 此时, $K=L$ 为交换群.

由上可知, G 的极大子群都是交换群或交换群, 从而 G 是类 3 的 $\mathcal{A}_2$ 群, 这与 G 的 $\mathcal{A}_2$ 子群都类 2 相矛盾. □

定理 6.2.1 的证明:

若 G 不是 $\mathcal{A}_2$ 群, 则由引理 6.2.2 可知 G 的 $\mathcal{A}_2$ 子群都是类 2 的. 再由引理 6.2.3 可知 $c(G)=2$, 矛盾. □

最后, 我们再给出一个简单的推论.

推论 6.2.4. *设 G 为导群初等交换的有限亚 Hamilton p 群, 且 $c(G)=3$, 则 $d(G)=2$ 且 p 为奇素数.*

证明 由定理 6.2.1, G 为 $\mathcal{A}_2$ 群. 再由推论 4.6.3 可得最终的结论. □

第七章　有限亚 Hamilton p 群的完全分类

在本章, 我们将完全分类有限亚 Hamilton p 群. 首先, 我们将有限亚 Hamilton p 群按照导群是否初等交换分为两类. 导群初等交换的时候, 由定理 6.2.1, 我们只需要解决幂零类为 2 的情形. 因为导群为 p 阶的群一定是亚 Hamilton p 群 (分类见文献 [20]), 我们只需要解决导群的阶大于 p 的情形.

§7.1　导群初等交换的有限亚 Hamilton p 群的分类

下面是本节的主要定理:

定理 7.1.1. *设 G 是有限 p 群, $c(G)=2$ 且 G' 是阶大于 p 的初等交换群, 则 G 是亚 Hamilton 群当且仅当 G 是以下互不同构的群之一:*

类型 (I): G' 为 p^2 阶初等交换群. G 有以下几种互不同构的类型:

(1) $G=K\times A$, 其中 $K=\langle a_1,a_2,a_3 \mid a_1^{p^{m_1}}=a_2^{p^{m_2+1}}=a_3^{p^{m_3+1}}=1,[a_1,a_2]=a_3^{p^{m_3}},[a_1,a_3]=a_2^{p^{m_2}},[a_2,a_3]=1\rangle$, $m_1\geqslant m_2=m_3+1$, A 是满足 $\exp(A)\leqslant p^{m_3}$ 的交换群;

(2) $G=K\times A$, 其中 $K=\langle a_1,a_2,a_3 \mid a_1^{p^{m_1}}=a_2^{p^{m_2+1}}=a_3^{p^{m_3+1}}=1,[a_1,a_2]=a_3^{p^{m_3}},[a_1,a_3]=a_2^{\nu p^{m_2}},[a_2,a_3]=1\rangle$, 其中 p 为奇素数, ν 是一个固定的模 p 的平方非剩余, $m_1\geqslant m_2=m_3+1$ 或者 $m_1\geqslant m_2=m_3$, A 是满足 $\exp(A)\leqslant p^{m_3}$ 的交换群;

(3) $G=K\times A$, 其中 $K=\langle a_1,a_2,a_3 \mid a_1^{p^{m_1}}=a_2^{p^{m_2+1}}=a_3^{p^{m_3+1}}=1,[a_1,a_2]=a_3^{p^{m_3}},[a_1,a_3]=a_2^{kp^{m_2}}a_3^{p^{m_3}},[a_2,a_3]=1\rangle$, 其中 $m_1\geqslant m_2=m_3$, 若 p 为奇素数, 则 $1+4k$ 是模 p 的平方非剩余; 若 $p=2$, 则 $k=1$. A 是满足 $\exp(A)\leqslant p^{m_3}$ 的交换群;

(4) $G=K\times A$, 其中 $K=\langle a_1,a_2,a_3 \mid a_1^{p^{m_1+1}}=a_2^{p^{m_2+1}}=a_3^{p^{m_3}}=1,[a_1,a_2]=a_1^{p^{m_1}},[a_1,a_3]=a_2^{p^{m_2}},[a_2,a_3]=1\rangle$, 其中 $m_1\geqslant m_2\geqslant m_3$. A 是满足 $\exp(A)\leqslant p^{m_2}$ 的交换群;

(5) $G=K\times A$, 其中 $K=\langle a_1,a_2,a_3 \mid a_1^{p^{m_1+1}}=a_2^{p^{m_2}}=a_3^{p^{m_3+1}}=1,[a_1,a_2]=a_3^{p^{m_3}},[a_1,a_3]=a_1^{p^{m_1}},[a_2,a_3]=1\rangle$, 其中 $m_1\geqslant m_2=m_3+1$. A 是满足 $\exp(A)\leqslant p^{m_3}$ 的交换群;

(6) $G = K \times A$. 其中 $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3}} = 1, [a_1, a_2] = 1, [a_1, a_3] = a_2^{p^{m_2}}, [a_2, a_3] = a_1^{p^{m_1}} \rangle$, 其中 $m_1 - 1 = m_2 \geqslant m_3$. A 是满足 $\exp(A) \leqslant p^{m_2}$ 的交换群;

(7) $G = K \times A$. 其中 $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3}} = 1, [a_1, a_2] = 1, [a_1, a_3] = a_2^{p^{m_2}}, [a_2, a_3] = a_1^{\nu p^{m_1}} \rangle$, 其中 p 为奇素数, ν 是一个固定的模 p 的平方非剩余, $m_1 - 1 = m_2 \geqslant m_3$ 或者 $m_1 = m_2 > m_3$, A 是满足 $\exp(A) \leqslant p^{m_2}$ 的交换群;

(8) $G = K \times A$. 其中 $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3}} = 1, [a_1, a_2] = 1, [a_1, a_3] = a_2^{p^{m_2}}, [a_2, a_3] = a_1^{kp^{m_1}} a_2^{-p^{m_2}} \rangle$, 其中 $m_1 = m_2 > m_3$, 若 p 为奇素数, 则 $1 + 4k$ 是模 p 的平方非剩余; 若 $p = 2$, 则 $k = 1$. A 是满足 $\exp(A) \leqslant p^{m_2}$ 的交换群;

(9) $G = K \times A$. 其中 $K = \langle a_1, a_2, b \mid a_1^4 = a_2^4 = 1, b^2 = a_1^2, [a_1, a_2] = 1, [a_1, b] = a_2^2, [a_2, b] = a_1^2 \rangle$, A 是满足 $\exp(A) \leqslant 2$ 的交换群;

(10) $G = K \times A$. 其中 $K = \langle a_1, a_2, b, d \mid a_1^4 = a_2^4 = 1, b^2 = a_1^2, d^2 = a_2^2, [a_1, a_2] = 1, [a_1, b] = a_2^2, [a_2, b] = a_1^2, [a_1, d] = a_1^2, [a_2, d] = a_1^2 a_2^2, [b, d] = 1 \rangle$, A 是满足 $\exp(A) \leqslant 2$ 的交换群.

类型 *(II)*: G' 为 p^3 阶初等交换群. G 有以下几种互不同构的类型:

(1a) $G = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3+1}} = 1, [a_1, a_2] = a_3^{p^{m_3}}, [a_1, a_3] = a_2^{\nu p^{m_2}}, [a_2, a_3] = a_1^{p^{m_1}} \rangle$, 其中 p 为奇素数, ν 是一个固定的模 p 的平方非剩余, $m_1 = m_2 = m_3 + 1$;

(1b) $G = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3+1}} = 1, [a_1, a_2] = a_3^{p^{m_3}}, [a_1, a_3] = a_1^{p^{m_1}} a_2^{lp^{m_2}}, [a_2, a_3] = a_1^{p^{m_1}} \rangle$, 其中 $m_1 = m_2 = m_3 + 1$. 若 $p = 2$, 则 $l = 1$; 若 $p > 2$, 则 $4l = g^{2r+1} - 1$, $r = 1, 2, \ldots, \frac{1}{2}(p-1)$, g 是模 p 的最小原根;

(2) $G = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3+1}} = 1, [a_1, a_2] = a_3^{p^{m_3}}, [a_1, a_3] = a_2^{\nu p^{m_2}}, [a_2, a_3] = a_1^{p^{m_1}} \rangle$, 其中 p 为奇素数, ν 是一个固定的模 p 的平方非剩余, $m_1 = m_2 + 1 = m_3 + 1$;

(3) $G = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3+1}} = 1, [a_1, a_2] = a_3^{p^{m_3}}, [a_1, a_3] = a_2^{kp^{m_2}} a_3^{-p^{m_3}}, [a_2, a_3] = a_1^{p^{m_1+1}} \rangle$, 其中 $m_1 = m_2 + 1 = m_3 + 1$, 若 p 为奇素数, 则 $1 + 4k$ 是模 p 的平方非剩余; 若 $p = 2$,

则 $k=1$;

(4) $G=\langle a_1,a_2,a_3 \mid a_1^4=a_2^4=a_3^4=1,[a_1,a_2]=a_3^2,[a_1,a_3]=a_2^2a_3^2,[a_2,a_3]=a_1^2a_2^2\rangle$.

本节的思路是: 由定理 7.1.2 和定理 7.1.5 完成定理 7.1.1 的充分性的证明; 由定理 7.1.4 和定理 7.1.7 完成定理 7.1.1 的必要性的证明.

定理 7.1.2. 下面的群都是有限亚 *Hamilton* p 群, $c(G)=2$. G' 为 p^2 阶初等交换 p 群. 不同类型是互不同构的, 同一类型对于不同的参数 (m_1,m_2,m_3) 或者不同的交换群 A 也是互不同构的. 为了研究方便, 我们把它们分为六种类型:

(Ia) $G=K\times A$. 其中 $K=\langle a_1,a_2,a_3 \mid a_1^{p^{m_1}}=a_2^{p^{m_2+1}}=a_3^{p^{m_3+1}}=1,[a_1,a_2]=a_3^{p^{m_3}},[a_1,a_3]=a_2^{p^{m_2}},[a_2,a_3]=1\rangle$, $m_1\geqslant m_2=m_3+1$, A 是满足 $\exp(A)\leqslant p^{m_3}$ 的交换群;

(Ib) $G=K\times A$. 其中 $K=\langle a_1,a_2,a_3 \mid a_1^{p^{m_1}}=a_2^{p^{m_2+1}}=a_3^{p^{m_3+1}}=1,[a_1,a_2]=a_3^{p^{m_3}},[a_1,a_3]=a_2^{\nu p^{m_2}},[a_2,a_3]=1\rangle$, 其中 p 为奇素数, ν 是一个固定的模 p 的平方非剩余, $m_1\geqslant m_2=m_3+1$ 或者 $m_1\geqslant m_2=m_3$, A 是满足 $\exp(A)\leqslant p^{m_3}$ 的交换群;

(Ic) $G=K\times A$. 其中 $K=\langle a_1,a_2,a_3 \mid a_1^{p^{m_1}}=a_2^{p^{m_2+1}}=a_3^{p^{m_3+1}}=1,[a_1,a_2]=a_3^{p^{m_3}},[a_1,a_3]=a_2^{kp^{m_2}}a_3^{-p^{m_3}},[a_2,a_3]=1\rangle$, 其中 $m_1\geqslant m_2=m_3$, 若 p 为奇素数, 则 $1+4k$ 是模 p 的平方非剩余; 若 $p=2$, 则 $k=1$. A 是满足 $\exp(A)\leqslant p^{m_3}$ 的交换群;

(II) $G=K\times A$. 其中 $K=\langle a_1,a_2,a_3 \mid a_1^{p^{m_1+1}}=a_2^{p^{m_2+1}}=a_3^{p^{m_3}}=1,[a_1,a_2]=a_1^{p^{m_1}},[a_1,a_3]=a_2^{p^{m_2}},[a_2,a_3]=1\rangle$, 其中 $m_1\geqslant m_2\geqslant m_3$. A 是满足 $\exp(A)\leqslant p^{m_2}$ 的交换群;

(III) $G=K\times A$. 其中 $K=\langle a_1,a_2,a_3 \mid a_1^{p^{m_1+1}}=a_2^{p^{m_2}}=a_3^{p^{m_3+1}}=1,[a_1,a_2]=a_3^{p^{m_3}},[a_1,a_3]=a_1^{p^{m_1}},[a_2,a_3]=1\rangle$. 其中 $m_1\geqslant m_2=m_3+1$. A 是满足 $\exp(A)\leqslant p^{m_3}$ 的交换群;

(IVa) $G=K\times A$. 其中 $K=\langle a_1,a_2,a_3 \mid a_1^{p^{m_1+1}}=a_2^{p^{m_2+1}}=a_3^{p^{m_3}}=1,[a_1,a_2]=1,[a_1,a_3]=a_2^{p^{m_2}},[a_2,a_3]=a_1^{p^{m_1}}\rangle$. 其中 $m_1-1=m_2\geqslant m_3$. A 是满足 $\exp(A)\leqslant p^{m_2}$ 的交换群;

(IVb) $G = K \times A$. 其中 $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3}} = 1, [a_1, a_2] = 1, [a_1, a_3] = a_2^{p^{m_2}}, [a_2, a_3] = a_1^{\nu p^{m_1}} \rangle$. 其中 p 为奇素数. ν 是一个固定的模 p 的平方非剩余. $m_1 - 1 = m_2 \geqslant m_3$ 或者 $m_1 = m_2 > m_3$, A 是满足 $\exp(A) \leqslant p^{m_2}$ 的交换群;

(IVc) $G = K \times A$. 其中 $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3}} = 1, [a_1, a_2] = 1, [a_1, a_3] = a_2^{p^{m_2}}, [a_2, a_3] = a_1^{kp^{m_1}} a_2{}^{p^{m_2}} \rangle$, 其中 $m_1 = m_2 > m_3$. 若 p 为奇素数, 则 $1 + 4k$ 是模 p 的平方非剩余; 若 $p = 2$, 则 $k = 1$. A 是满足 $\exp(A) \leqslant p^{m_2}$ 的交换群;

(V) $G = K \times A$. 其中 $K = \langle a_1, a_2, b \mid a_1^4 = a_2^4 = 1, b^2 = a_1^2, [a_1, a_2] = 1, [a_1, b] = a_2^2, [a_2, b] = a_1^2 \rangle$. A 是满足 $\exp(A) \leqslant 2$ 的交换群;

(VI) $G = K \times A$. 其中 $K = \langle a_1, a_2, b, d \mid a_1^4 = a_2^4 = 1, b^2 = a_1^2, d^2 = a_2^2, [a_1, a_2] = 1, [a_1, b] = a_2^2, [a_2, b] = a_1^2, [a_1, d] = a_1^2, [a_2, d] = a_1^2 a_2^2, [b, d] = 1 \rangle$, A 是满足 $\exp(A) \leqslant 2$ 的交换群.

证明 我们首先证明定理中的群都是有限亚 Hamilton p 群. 先来看 (V) 型群和 (VI) 型群, 即定理 5.2.4 中的 (2) 型群和 (3) 型群. 由于 G 的每个二元生成的非交换子群 N 都与 $M_2(2, 2)$ 同构, 我们有 $|\mho_1(N)| = 4$. 注意到 $\mho_1(G) = G'$ 亦为 4 阶初等交换群, 我们有 $G' = \mho_1(N)$. 从而 $N \trianglelefteq G$. 再由定理 6.1.1 可知 G 为有限亚 Hamilton p 群.

下面我们分别证明其它类型的群的二元生成的非交换子群也都正规, 从而由定理 6.1.1 可知 G 为有限亚 Hamilton p 群. 对于这些群, 我们都有 $Z(G) = \Phi(K) \times A$, 从而 G 的所有二元生成的非交换子群只可能为以下几种: 第一种, $N = \langle a_1 a_2^i x, a_3 y \rangle$, 其中 $x, y \in Z(G)$; 第二种, $N = \langle a_1 a_3^j x, a_2 a_3^k y \rangle$, 其中 $x, y \in Z(G)$; 第三种, $N = \langle a_2 x, a_3 y \rangle$, 其中 $x, y \in Z(G)$.

(Ia) 型群的讨论:

第一种, $N = \langle a_1 a_2^i x, a_3 y \rangle$, 其中 $x, y \in Z(G)$. 此时, $N' = \langle a_2^{p^{m_2}} \rangle$. 计算可得对于 $z \in Z(G)$ 有 $z^{p^{m_2}} \in \langle a_1^{p^{m_2+1}} \rangle$. 因为 $a_1^{p^{m_2}} x^{p^{m_2}} = (a_1 a_2^i x)^{p^{m_2}} a_2^{-ip^{m_2}} \in N$, 所以有 $a_1^{p^{m_2}} \in N$ 和 $z^{p^{m_2}} \in N$. 又因为 $y^{p^{m_3}} \in \langle a_2^{p^{m_2}}, a_1^{p^{m_2}} \rangle$, 所以 $y^{p^{m_3}} \in N$, 从而 $a_3^{p^{m_3}} = (a_3 y)^{p^{m_3}} y^{-p^{m_3}} \in N$. 这说明 $G' \leqslant N$, 从而 $N \trianglelefteq G$.

第二种, $N = \langle a_1 a_3^j x, a_2 a_3^k y \rangle$, 其中 $x, y \in Z(G)$. 此时, $N' = \langle a_2^{kp^{m_2}} a_3^{p^{m_3}} \rangle$. 计算可得对于 $z \in Z(G)$ 有 $z^{p^{m_2}} \in \langle a_1^{p^{m_2+1}} \rangle$. 因为 $a_1^{p^{m_2}} x^{p^{m_2}} = (a_1 a_3^j x)^{p^{m_2}} \in$

N, 所以有 $a_1^{p^{m_2}} \in N$ 和 $z^{p^{m_2}} \in N$. 进而 $a_2^{p^{m_2}} = (a_2a_3^ky)^{p^{m_2}}y^{-p^{m_2}} \in N$. 这说明 $G' \leqslant N$, 从而 $N \trianglelefteq G$.

第三种, $N = \langle a_2x, a_3y\rangle$, 其中 $x, y \in Z(G)$. 对于 (I) 型群, N 是交换群.

(Ib) 型群的讨论:

第一种, $N = \langle a_1a_2^ix, a_3y\rangle$, 其中 $x, y \in Z(G)$. 此时, $N' = \langle a_2^{p^{m_2}}\rangle$. 计算可得对于 $z \in Z(G)$ 有 $z^{p^{m_2}} \in \langle a_1^{p^{m_2+1}}\rangle$. 因为 $a_1^{p^{m_2}}x^{p^{m_2}} = (a_1a_2^ix)^{p^{m_2}}a_2^{-ip^{m_2}} \in N$, 所以有 $a_1^{p^{m_2}} \in N$ 和 $z^{p^{m_2}} \in N$. 又因为 $y^{p^{m_3}} \in \langle a_2^{p^{m_3+1}}, a_1^{p^{m_3+1}}\rangle \leqslant N$, 所以 $y^{p^{m_3}} \in N$. 从而 $a_3^{p^{m_3}} = (a_3y)^{p^{m_3}}y^{-p^{m_3}} \in N$. 这说明 $G' \leqslant N$, 从而 $N \trianglelefteq G$.

第二种, $N = \langle a_1a_3^jx, a_2a_3^ky\rangle$, 其中 $x, y \in Z(G)$. 此时, $N' = \langle a_2^{k\nu p^{m_2}}a_3^{p^{m_3}}\rangle$. (i) 若 $m_1 \geqslant m_2 = m_3 + 1$, 计算可得对于 $z \in Z(G)$ 有 $z^{p^{m_2}} \in \langle a_1^{p^{m_2+1}}\rangle$. 因为 $a_1^{p^{m_2}}x^{p^{m_2}} = (a_1a_3^jx)^{p^{m_2}} \in N$, 所以有 $a_1^{p^{m_2}} \in N$ 和 $z^{p^{m_2}} \in N$. 进而 $a_2^{p^{m_2}} = (a_2a_3^ky)^{p^{m_2}}y^{-p^{m_2}} \in N$. 这说明 $G' \leqslant N$, 从而 $N \trianglelefteq G$. (ii) 若 $m_1 \geqslant m_2 = m_3$, 计算可得对于 $z \in Z(G)$ 有 $z^{p^{m_2}} \in \langle a_1^{p^{m_2+1}}\rangle$. 因为 $a_1^{p^{m_2+1}}x^{p^{m_2+1}} = (a_1a_3^jx)^{p^{m_2+1}} \in N$, 所以有 $a_1^{p^{m_2+1}} \in N$ 和 $z^{p^{m_2}} \in N$. 进而 $a_2^{p^{m_2}}a_3^{kp^{m_3}} = (a_2a_3^ky)^{p^{m_2}}y^{-p^{m_2}} \in N$. 这说明 $\langle a_2^{p^{m_2}}a_3^{kp^{m_3}}, a_2^{k\nu p^{m_2}}a_3^{p^{m_3}}\rangle \leqslant N$. 由于 ν 是一个模 p 的平方非剩余, $G' = \langle a_2^{p^{m_2}}, a_3^{p^{m_3}}\rangle = \langle a_2^{p^{m_2}}a_3^{kp^{m_3}}, a_2^{k\nu p^{m_2}}a_3^{p^{m_3}}\rangle \leqslant N$, 从而 $N \trianglelefteq G$.

第三种, $N = \langle a_2x, a_3y\rangle$, 其中 $x, y \in Z(G)$. 对于 (I) 型群, N 是交换群.

(Ic) 型群的讨论:

第一种, $N = \langle a_1a_2^ix, a_3y\rangle$, 其中 $x, y \in Z(G)$. 此时, $N' = \langle a_2^{kp^{m_2}}a_3^{-p^{m_3}}\rangle$. 计算可得对于 $z \in Z(G)$ 有 $z^{p^{m_2}} \in \langle a_1^{p^{m_2+1}}\rangle$. 因为

$$a_1^{p^{m_2+1}}x^{p^{m_2+1}} = (a_1a_2^ix)^{p^{m_2+1}} \in N,$$

所以有 $a_1^{p^{m_2+1}} \in N$ 和 $z^{p^{m_2}} \in N$. 又因为 $y^{p^{m_3}} = y^{p^{m_2}} \in \langle a_1^{p^{m_2+1}}\rangle$, 所以 $y^{p^{m_3}} \in N$, 从而 $a_3^{p^{m_3}} = (a_3y)^{p^{m_3}}y^{-p^{m_3}} \in N$. 这说明 $G' \leqslant N$, 从而 $N \trianglelefteq G$.

第二种, $N = \langle a_1a_3^ix, a_2a_3^jy\rangle$, 其中 $x, y \in Z(G)$. 此时,

$$N' = \langle a_2^{jkp^{m_2}}a_3^{(1-j)p^{m_3}}\rangle.$$

计算可得对于 $z \in Z(G)$ 有 $z^{p^{m_2}} \in \langle a_1^{p^{m_2+1}}\rangle$. 因为

$$a_1^{p^{m_2+1}}x^{p^{m_2+1}} = (a_1a_3^jx)^{p^{m_2+1}} \in N,$$

所以有 $a_1^{p^{m_2+1}} \in N$ 和 $z^{p^{m_2}} \in N$. 进而 $a_2^{p^{m_2}} a_3^{jp^{m_3}} = (a_2a_3^j y)^{p^{m_2}} y^{-p^{m_2}} \in N$. 这说明 $\langle a_2^{p^{m_2}} a_3^{jp^{m_3}}, a_2^{jkp^{m_2}} a_3^{(1-j)p^{m_3}} \rangle \leqslant N$. 不论是 $p=2$ 且 $k=1$, 还是 $1+4k$ 为模 p(奇素数) 的平方非剩余, 关于 j 的同余方程 $kj^2+j-1 \equiv 0 \pmod p$ 都无解. 这说明 $G' = \langle a_2^{p^{m_2}}, a_3^{p^{m_3}} \rangle = \langle a_2^{p^{m_2}} a_3^{jp^{m_3}}, a_2^{jkp^{m_2}} a_3^{(1-j)p^{m_3}} \rangle \leqslant N$, 从而 $N \trianglelefteq G$.

第三种, $N = \langle a_2x, a_3y \rangle$, 其中 $x, y \in Z(G)$. 对于 (I) 型群, N 是交换群.

(II) 型群的讨论:

第一种, $N = \langle a_1a_2^i x, a_3y \rangle$, 其中 $x, y \in Z(G)$. 此时, $N' = \langle a_2^{p^{m_2}} \rangle$. 因为 $a_1^{p^{m_1}} = (a_1a_2^i x)^{p^{m_1}} a_2^{-ip^{m_1}} \in N$, 所以 $G' \leqslant N$, 从而 $N \trianglelefteq G$.

第二种, $N = \langle a_1a_3^j x, a_2a_3^k y \rangle$, 其中 $x, y \in Z(G)$. 此时, $N' = \langle a_1^{p^{m_1}} a_2^{kp^{m_2}} \rangle$. 因为 $a_2^{p^{m_2}} = (a_2a_3^k y)^{p^{m_2}} \in N$, 所以 $G' \leqslant N$, 从而 $N \trianglelefteq G$.

第三种, $N = \langle a_2x, a_3y \rangle$, 其中 $x, y \in Z(G)$. 对于 (II) 型群, N 也是交换群.

(III) 型群的讨论:

第一种, $N = \langle a_1a_2^i x, a_3y \rangle$, 其中 $x, y \in Z(G)$. 此时, $N' = \langle a_1^{p^{m_1}} \rangle$, 且对所有的 $z \in Z(G)$ 有 $z^{p^{m_3}} \in \langle a_1^{p^{m_2}} \rangle$. 因为 $a_1^{p^{m_2}} x^{p^{m_3+1}} = a_1^{p^{m_2}} x^{p^{m_2}} = (a_1a_2^i x)^{p^{m_2}} \in N$, 所以有 $a_1^{p^{m_2}} \in N$ 和 $z^{p^{m_3}} \in N$, 从而 $a_3^{p^{m_3}} = (a_3y)^{p^{m_3}} y^{-p^{m_3}} \in N$. 这说明 $G' \leqslant N$, 从而 $N \trianglelefteq G$.

第二种, $N = \langle a_1a_3^j x, a_2a_3^k y \rangle$, 其中 $x, y \in Z(G)$. 此时, $N' = \langle a_3^{p^{m_3}} a_1^{kp^{m_1}} \rangle$. 因为 $a_1^{p^{m_1}} = (a_1a_3^j x)^{p^{m_1}} \in N$, 所以 $G' \leqslant N$, 从而 $N \trianglelefteq G$.

第三种, $N = \langle a_2x, a_3y \rangle$, 其中 $x, y \in Z(G)$. 对于 (III) 型群, N 也是交换群.

(IVa) 型群的讨论:

第一种, $N = \langle a_1a_2^i x, a_3y \rangle$, 其中 $x, y \in Z(G)$. 此时, $N' = \langle a_2^{p^{m_2}} a_1^{ip^{m_1}} \rangle$. 因为 $a_1^{p^{m_1}} = (a_1a_2^i x)^{p^{m_1}} \in N$, 所以 $G' \leqslant N$, 从而 $N \trianglelefteq G$.

第二种, $N = \langle a_1a_3^j x, a_2a_3^k y \rangle$, 其中 $x, y \in Z(G)$. 此时, $N' = \langle a_2^{kp^{m_2}} a_1^{-jp^{m_1}} \rangle$. 易知 $a_1^{p^{m_1}} = (a_1a_3^j x)^{p^{m_1}} \in N$. 所以若 $(k, p) = 1$, 则有 $G' \leqslant N$, 从而 $N \trianglelefteq G$. 若 $N = \langle a_1a_3^j x, a_2y \rangle$, 由于对所有的 $z \in Z(G)$ 都有 $z^{p^{m_2}} \in \langle a_1^{p^{m_2+1}} \rangle$, 以及 $a_1^{p^{m_2+1}} x^{p^{m_2+1}} = (a_1a_2^i x)^{p^{m_2+1}} \in N$, 我们有 $a_1^{p^{m_2+1}} \in N$ 和 $z^{p^{m_2}} \in N$, 从而 $a_2^{p^{m_2}} = (a_2y)^{p^{m_2}} y^{-p^{m_2}} \in N$. 所以仍然有 $G' \leqslant N$, 从而 $N \trianglelefteq G$.

第三种, $N = \langle a_2x, a_3y \rangle$, 其中 $x, y \in Z(G)$. 此时 $N' = \langle a_1^{p^{m_1}} \rangle$. 因为 $x^{p^{m_2}} \in \langle a_1^{p^{m_1}} \rangle$, 所以 $a_2^{p^{m_2}} = (a_2x)^{p^{m_2}} x^{-p^{m_2}} \in N$. 这说明 $G' \leqslant N$, 从而

$N \trianglelefteq G$.

(IVb) 型群的讨论:

第一种, $N = \langle a_1a_2^ix, a_3y\rangle$, 其中 $x, y \in Z(G)$. 此时, $N' = \langle a_2^{p^{m_2}}a_1^{i\nu p^{m_1}}\rangle$. 若 $m_1 > m_2$ 或者 $N = \langle a_1x, a_3y\rangle$, 则 $a_1^{p^{m_1}} = (a_1a_2^ix)^{p^{m_1}} \in N$. 此时 $G' \leqslant N$, 从而 $N \trianglelefteq G$; 若 $m_1 = m_2$ 且 $(i, p) = 1$, 因为 $a_1^{p^{m_1}}a_2^{ip^{m_2}} = (a_1a_2^ix)^{p^{m_1}} \in N$, 所以 $a_2^{(1-i^2\nu)p^{m_2}} = (a_2^{p^{m_2}}a_1^{i\nu p^{m_1}})(a_1^{p^{m_1}}a_2^{ip^{m_1}})^{-i\nu} \in N$. 由于 ν 是一个模 p 的平方非剩余, 我们有 $a_2^{p^{m_2}} \in N$. 此时, $G' \leqslant N$, 从而 $N \trianglelefteq G$.

第二种, $N = \langle a_1a_3^jx, a_2a_3^ky\rangle$, 其中 $x, y \in Z(G)$. 此时,

$$N' = \langle a_2^{kp^{m_2}}a_1^{-j\nu p^{m_1}}\rangle.$$

易知 $a_1^{p^{m_1}} = (a_1a_3^jx)^{p^{m_1}} \in N$. 所以若 $(k, p) = 1$, 则有 $G' \leqslant N$, 从而 $N \trianglelefteq G$. 若 $N = \langle a_1a_3^jx, a_2y\rangle$, 由于对所有的 $z \in Z(G)$ 有 $z^{p^{m_2}} \in \langle a_1^{p^{m_2+1}}\rangle$, 以及 $a_1^{p^{m_2+1}}x^{p^{m_2+1}} = (a_1a_2^ix)^{p^{m_2+1}} \in N$, 我们有 $a_1^{p^{m_2+1}} \in N$ 和 $z^{p^{m_2}} \in N$, 从而 $a_2^{p^{m_2}} = (a_2y)^{p^{m_2}}y^{-p^{m_2}} \in N$. 所以仍然有 $G' \leqslant N$, 从而 $N \trianglelefteq G$.

第三种, $N = \langle a_2x, a_3y\rangle$, 其中 $x, y \in Z(G)$. 此时 $N' = \langle a_1^{p^{m_1}}\rangle$. 因为 $x^{p^{m_2}} \in \langle a_1^{p^{m_1}}\rangle$, 所以 $a_2^{p^{m_2}} = (a_2x)^{p^{m_2}}x^{-p^{m_2}} \in N$. 这说明 $G' \leqslant N$, 从而 $N \trianglelefteq G$.

(IVc) 型群的讨论:

第一种, $N = \langle a_1a_2^ix, a_3y\rangle$, 其中 $x, y \in Z(G)$. 此时, $N' = \langle a_2^{(1-i)p^{m_2}}a_1^{ikp^{m_1}}\rangle$. 因为 $a_1^{p^{m_1}}a_2^{ip^{m_2}} = (a_1a_2^ix)^{p^{m_1}} \in N$, 所以 $\langle a_2^{(1-i)p^{m_2}}a_1^{ikp^{m_1}}, a_1^{p^{m_1}}a_2^{ip^{m_2}}\rangle \leqslant N$. 此时, 不论 $p = 2$ 且 $k = 1$ 还是 $1 + 4k$ 是模 p(奇素数) 的平方非剩余, 关于 i 的二次同余方程 $i^2k + i - 1 \equiv 0 \pmod p$ 都无解. 这说明 $G' = \langle a_2^{(1-i)p^{m_2}}a_1^{ikp^{m_1}}, a_1^{p^{m_1}}a_2^{ip^{m_2}}\rangle \leqslant N$, 从而 $N \trianglelefteq G$.

第二种, $N = \langle a_1a_3^ix, a_2a_3^jy\rangle$, 其中 $x, y \in Z(G)$. 此时, 易知 $a_1^{p^{m_1}} = (a_1a_3^ix)^{p^{m_1}} \in N$, 并且 $a_2^{p^{m_2}} = (a_2a_3^jy)^{p^{m_2}} \in N$. 所以仍然有 $G' \leqslant N$, 从而 $N \trianglelefteq G$.

第三种, $N = \langle a_2x, a_3y\rangle$, 其中 $x, y \in Z(G)$. 此时 $N' = \langle a_1^{kp^{m_1}}a_2^{-p^{m_2}}\rangle$. 因为 $x^{p^{m_2}} = 1$, 所以 $a_2^{p^{m_2}} = (a_2x)^{p^{m_2}} \in N$. 这说明 $G' \leqslant N$, 从而 $N \trianglelefteq G$.

下面我们说明这些群都是互不同构的.

首先, 因为 (VI) 型群是唯一的一种没有交换极大子群的群, 所以与其它类型的群不同构. 在剩下的满足 G/G' 为初等交换 2 群的群中, (V) 型群是唯一的

2 阶元都在中心的群, 所以 (V) 型群也与其他类型互不同构.

余下的群都有 $G/G' \cong \langle \bar{a}_1 \rangle \times \langle \bar{a}_2 \rangle \times B$. 其中 $o(\bar{a}_1) = p^{m_1}$, $o(\bar{a}_2) = p^{m_2}$, B 是满足 $\exp(B) \leqslant p^{m_2}$ 的交换群. 可见, 如果有两个群同构, 必有相同的参数 m_1 和 m_2. 另一方面, 在余下的群中 K 都是满足 $K' = G'$ 的 G 的最小阶的一个子群. 所以如果有两个群同构, 必有相同的参数 m_1、m_2 和 m_3. 再考虑 G/G' 的型不变量, 如果有两个群同构, 还必有同构的交换群 A.

若 $m_1 > m_2$, 由于 (I) 型群中 $\exp(G) = p^{m_1}$, 而其它群中都有 $\exp(G) = p^{m_1+1}$, 所以 (I) 型群其它群不同构. 由于 (IV) 型群中的交换极大子群

$$M = \langle a_1, a_2, Z(G) \rangle$$

满足 $\exp(M) = p^{m_1}$, 而其它群中的交换极大子群 $M = \langle a_2, a_3, Z(G) \rangle$ 满足 $\exp(M) < p^{m_1}$, 所以 (IV) 型群其它群不同构. 由于 (II) 型群满足 $G' \leqslant \mho_{m_2}(G)$, 而 (III) 型群满足 $\mho_{m_2}(G) = \langle a_1^{p^{m_2}} \rangle$, 所以 (II) 型群和 (III) 型群也不同构.

若 $m_1 = m_2 > m_3$, 先考虑 $\mho_{m_3}(G)$. 对于 (I) 或 (III) 型群 $\mho_{m_3}(G)$ 是三元生成的, 对于 (II) 或 (IV) 型群, 当 $\exp(A) \leqslant p^{m_3}$ 时 $\mho_{m_3}(G)$ 是二元生成的, 所以 (I) 型群和 (III) 型群分别与 (II) 型群和 (IV) 型群不同构 (注意, 若 (II) 型群或 (IV) 型群与 (I) 型群或 (III) 型群同构, 则一定有 $\exp(A) \leqslant p^{m_3}$). 由于 (I) 型群中的交换极大子群 $M = \langle a_2, a_3, Z(G) \rangle$ 满足 $\exp(M) = p^{m_2+1}$, 而 (III) 型群中的交换极大子群 $M = \langle a_2, a_3, Z(G) \rangle$ 满足 $\exp(M) = p^{m_2}$, 所以 (I) 型群和 (III) 型群也不同构. 再考虑 (II) 型群和 (IV) 型群中交换极大子群的型不变量, 可知 (II) 型群和 (IV) 型群也不同构.

若 $m_1 = m_2 = m_3$, 也可由交换极大子群的型不变量得出 (I) 型群和 (II) 型群互不同构 (注意, 这种情况下没有 (III) 型群和 (IV) 型群).

最后我们还剩下四种情况:

(1) $m_1 \geqslant m_2 = m_3 + 1$ 时, (Ia) 型群和 (Ib) 型群互不同构.

设 $G = \langle a_1, a_2, a_3, A \rangle$ 为一个 (Ia) 型群, $\bar{G} = \langle \bar{a}_1, \bar{a}_2, \bar{a}_3, \bar{A} \rangle$ 为一个 (Ib) 型群. 若 $\bar{G}$ 与 G 同构, 我们设 θ 是一个从 $\bar{G}$ 到 G 的同构映射. 因为 $M = \langle a_2, a_3, A, a_1^p \rangle$、$Z(G)$ 以及 $\bar{M} = \langle \bar{a}_2, \bar{a}_3, \bar{A}, \bar{a}_1^p \rangle$、$Z(\bar{G})$ 是 G 或 $\bar{G}$ 的特征子群, 我们有 $\bar{M}^\theta = M$ 和 $Z(\bar{G})^\theta = Z(G)$. 从而, 我们可设 $\bar{a}_1^\theta = a_1^i x$, $\bar{a}_2^\theta = a_2^j a_3^k y$, $\bar{a}_3^\theta = a_3^s z$, 其中 $x \in M$、$y, z \in Z(G)$, i, j, s 都与 p 互素.

由 $[\bar{a}_1^\theta, \bar{a_2}^\theta] = [\bar{a}_1, \bar{a_2}]^\theta = (\bar{a_3}^{p^{m_3}})^\theta$ 可得, $[a_1^i x, a_2^j a_3^k y] = (a_3^s z)^{p^{m_3}}$, 即 $a_3^{ijp^{m_3}} a_2^{ikp^{m_2}} = a_3^{sp^{m_3}} z^{p^{m_3}}$. 比较指数可得 $s \equiv ij \pmod p$.

再由 $[\bar{a}_1^\theta, \bar{a_3}^\theta] = [\bar{a}_1, \bar{a_3}]^\theta = (\bar{a_2}^{\nu p^{m_2}})^\theta$ 可得, $[a_1^i x, a_3^s z] = (a_2^j a_3^k y)^{p^{m_2}}$, 即 $a_2^{isp^{m_2}} = a_2^{j\nu p^{m_2}} y^{p^{m_3}}$. 比较指数可得 $j\nu \equiv is \pmod p$. 将 $s \equiv ij \pmod p$ 代入可得 $j\nu \equiv i^2 j \pmod p$, 这与 ν 是一个模 p 的平方非剩余矛盾.

(2) $m_1 \geqslant m_2 = m_3$ 时, (Ib) 型群和 (Ic) 型群互不同构, 并且 (Ic) 型群取不同的参数 k 也互不同构.

我们只需要处理 p 为奇素数的情形. 设 $m_2 = m_3 = m$, 将这两种类型群中的 K 用统一的形式写成: $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1}} = a_2^{p^{m+1}} = a_3^{p^{m+1}} = 1, [a_1, a_2] = a_3^{p^m}, [a_1, a_3] = a_2^{jp^m} a_3^{ip^m}, [a_2, a_3] = 1\rangle$, 其中 $i^2 + 4j$ 是模 p 的平方非剩余.

设 $G = \langle a_1, a_2, a_3, A\rangle$ 和 $\bar{G} = \langle \bar{a}_1, \bar{a}_2, \bar{a}_3, \bar{A}\rangle$ 是满足以上条件的两个群, 参数分别为 (j, i) 和 (j', i'). 若 $\bar{G}$ 与 G 同构, 我们设 θ 是一个从 $\bar{G}$ 到 G 的同构映射. 因为 $M = \langle a_2, a_3, A, a_1^p\rangle$, $Z(G)$ 以及 $\bar{M} = \langle \bar{a}_2, \bar{a}_3, \bar{A}, \bar{a}_1^p\rangle$, $Z(\bar{G})$ 是 G 或 $\bar{G}$ 的特征子群, 我们有 $\bar{M}^\theta = M$ 和 $Z(\bar{G})^\theta = Z(G)$. 从而, 我们可设 $\bar{a}_1^\theta = a_1^t x$, $\bar{a}_2^\theta = a_2^r a_3^s y$, $\bar{a}_3^\theta = a_2^u a_3^v z$, 其中 $x \in M$, $y, z \in Z(G)$, $t, rv - us$ 都与 p 互素.

由 $[\bar{a}_1^\theta, \bar{a_2}^\theta] = [\bar{a}_1, \bar{a_2}]^\theta = (\bar{a_3}^{p^m})^\theta$ 可得

$$[a_1^t x, a_2^r a_3^s y] = (a_2^u a_3^v z)^{p^m}$$

即 $a_2^{tsjp^m} a_3^{(tsi+tr)p^m} = a_2^{up^m} a_3^{vp^m} z^{p^m}$. 比较指数可得

$$u \equiv tsj \pmod p, v \equiv tsi + tr \pmod p. \tag{1}$$

再由 $[\bar{a}_1^\theta, \bar{a_3}^\theta] = [\bar{a}_1, \bar{a_3}]^\theta = (\bar{a_2}^{j'p^m} \bar{a}_3^{i'p^m})^\theta$ 可得

$$[a_1^t x, a_2^u a_3^v z] = (a_2^r a_3^s y)^{j'p^m} (a_2^u a_3^v z)^{i'p^m}.$$

即 $a_2^{jtvp^m} a_3^{(itv+tu)p^m} = a_2^{(rj'+ui')p^m} a_3^{(sj'+vi')p^m} y^{j'p^{m_3}} z^{i'p^m}$. 比较指数可得到以下式子,

$$\begin{cases} rj' + ui' \equiv jtv \pmod p \\ sj' + vi' \equiv itv + tu \pmod p \end{cases} \tag{2}$$

由 (2) 解得,

$$\begin{vmatrix} r & u \\ s & v \end{vmatrix} j' \equiv \begin{vmatrix} jtv & u \\ tu + itv & v \end{vmatrix} \pmod p$$

$$\begin{vmatrix} r & u \\ s & v \end{vmatrix} i' \equiv \begin{vmatrix} r & jtv \\ s & tu+itv \end{vmatrix} \pmod p$$

将 (1) 代入, 有

$$\begin{aligned}(rv-su)j' &\equiv jtv^2 - tu^2 - ituv \pmod p\\ &\equiv jtv(tsi+tr) - tu(tsj) - it(tsj)v\\ &= (rv-su)jt^2\end{aligned}$$

$$\begin{aligned}(rv-su)i' &\equiv rtu + ritv - sjtv \pmod p\\ &\equiv rtu + ritv - uv\\ &\equiv rtu + ritv - u(tsi+tr)\\ &= (rv-su)it\end{aligned}$$

由于 $(rv-su,p)=1$, 我们有 $j' \equiv jt^2 \pmod p$ 和 $i' \equiv it \pmod p$.

因为 (Ib) 型群的参数 (j,i) 为 $(\nu,0)$, 而 (Ic) 型群的参数 (j',i') 为 $(k,-1)$, 不满足上述条件, 所以 (Ib) 型群和 (Ic) 型群不同构. 容易看出, 当 $i=i'$ 时, 满足上述条件的参数也一定满足 $j' \equiv j \pmod p$, 所以两个不同参数 k 的 (Ic) 型群也互不同构.

(3) $m_1 - 1 = m_2 \geqslant m_3$ 时, (IVa) 型群和 (IVb) 型群互不同构.

设 $G = \langle a_1, a_2, a_3, A\rangle$ 为一个 (IVa) 型群, $\bar{G} = \langle \bar{a}_1, \bar{a}_2, \bar{a}_3, \bar{A}\rangle$ 为一个 (IVb) 型群. 若 $\bar{G}$ 与 G 同构, 我们设 θ 是一个从 $\bar{G}$ 到 G 的同构映射. 因为 $M = \langle a_1, a_2, A, a_3^p\rangle$, $Z(G)$ 以及 $\bar{M} = \langle \bar{a}_1, \bar{a}_2, \bar{A}, \bar{a}_3^p\rangle$, $Z(\bar{G})$ 是 G 或 $\bar{G}$ 的特征子群, 我们有 $\bar{M}^\theta = M$ 和 $Z(\bar{G})^\theta = Z(G)$. 从而, 我们可设 $\bar{a}_1^\theta = a_1^i a_2^r x$, $\bar{a}_2^\theta = a_2^j a_1^{kp} y$, $\bar{a}_3^\theta = a_3^s z$, 其中 $y \in \Omega_{m_2}(M)$, $x, z \in Z(G)$, i, j, s 都与 p 互素.

由 $[\bar{a}_1^\theta, \bar{a_3}^\theta] = [\bar{a}_1, \bar{a_3}]^\theta = (\bar{a_2}^{p^{m_2}})^\theta$ 可得

$$[a_1^i a_2^r x, a_3^s z] = (a_2^j a_1^{kp} y)^{p^{m_2}}.$$

即 $a_1^{rs\nu p^{m_1}} a_2^{isp^{m_2}} = a_1^{kp^{m_1}} a_2^{jp^{m_2}}$. 比较指数可得 $rs \equiv k \pmod p$ 和 $is \equiv j \pmod p$.

再由 $[\bar{a}_2^\theta, \bar{a_3}^\theta] = [\bar{a}_2, \bar{a_3}]^\theta = (\bar{a_1}^{\nu p^{m_1}})^\theta$ 可得

$$[a_2^j a_1^{kp} y, a_3^s z] = (a_1^i a_2^r x)^{\nu p^{m_1}}.$$

即 $a_1^{jsp^{m_1}}=a_1^{i\nu p^{m_1}}$. 比较指数可得 $js\nu\equiv i\nu \pmod p$. 将 $is\equiv j \pmod p$ 代入可得 $is^2\nu\equiv i \pmod p$, 这与 ν 是一个模 p 的平方非剩余矛盾.

(4) $m_1=m_2>m_3$ 时, (IVb) 型群和 (IVc) 型群互不同构, 并且 (IVc) 型群取不同的参数 k 也互不同构.

我们只需要处理 p 为奇素数的情形. 设 $m_1=m_2=m$, 将这两种类型群中的 K 用统一的形式写成: $K=\langle a_1,a_2,a_3 \mid a_1^{p^{m+1}}=a_2^{p^{m+1}}=a_3^{p^{m_3}}=1,[a_1,a_2]=1,[a_2,a_3]=a_2^{p^m},[a_1,a_3]=a_1^{jp^m}a_2^{ip^m}\rangle$, 其中 i^2+4j 是模 p 的平方非剩余.

设 $G=\langle a_1,a_2,a_3,A\rangle$ 和 $\bar{G}=\langle \bar{a}_1,\bar{a}_2,\bar{a}_3,\bar{A}\rangle$ 是满足以上条件的两个群, 参数分别为 (j,i) 和 (j',i'). 若 $\bar{G}$ 与 G 同构, 我们设 θ 是一个从 $\bar{G}$ 到 G 的同构映射. 因为 $M=\langle a_1,a_2,A,a_3^p\rangle$, $Z(G)$ 以及 $\bar{M}=\langle \bar{a}_1,\bar{a}_2,\bar{A},\bar{a}_3^p\rangle$, $Z(\bar{G})$ 是 G 或 $\bar{G}$ 的特征子群, 我们有 $\bar{M}^\theta=M$ 和 $Z(\bar{G})^\theta=Z(G)$. 从而, 我们可设 $\bar{a}_3^\theta=a_3^tx$, $\bar{a}_1^\theta=a_1^ra_2^sy$, $\bar{a}_2^\theta=a_1^ua_2^uz$, 其中 $x\in M$, $y,z\in Z(G)$, $t,rv-us$ 都与 p 互素.

由 $[\bar{a}_1^\theta,\bar{a_3}^\theta]=[\bar{a}_1,\bar{a_3}]^\theta=(\bar{a_2}^{p^m})^\theta$ 可得

$$[a_1^ra_2^sy,a_3^tx]=(a_1^ua_2^vz)^{p^m}.$$

即 $a_1^{tsjp^m}a_2^{(tsi+tr)p^m}=a_1^{up^m}a_2^{vp^m}$. 比较指数可得

$$u\equiv tsj \pmod p, v\equiv tsi+tr \pmod p. \tag{3}$$

再由 $[\bar{a}_2^\theta,\bar{a_3}^\theta]=[\bar{a}_2,\bar{a_3}]^\theta=(\bar{a_1}^{j'p^m}\bar{a}_2^{i'p^m})^\theta$ 可得

$$[a_1^ua_2^vz,a_3^tx]=(a_1^ra_2^sy)^{j'p^m}(a_1^ua_2^vz)^{i'p^m}.$$

即 $a_1^{jtvp^m}a_2^{(itv+tu)p^m}=a_1^{(rj'+ui')p^m}a_2^{(sj'+vi')p^m}$. 比较指数可得到以下式子,

$$\begin{cases} rj'+ui'\equiv jtv \pmod p \\ sj'+vi'\equiv itv+tu \pmod p \end{cases} \tag{4}$$

由 (4) 解得,

$$\begin{vmatrix} r & u \\ s & v \end{vmatrix} j'\equiv \begin{vmatrix} jtv & u \\ tu+itv & v \end{vmatrix} \pmod p$$

$$\begin{vmatrix} r & u \\ s & v \end{vmatrix} i'\equiv \begin{vmatrix} r & jtv \\ s & tu+itv \end{vmatrix} \pmod p$$

将 (3) 代入, 有

$$\begin{aligned}(rv-su)j' &\equiv jtv^2-tu^2-ituv \pmod p\\ &\equiv jtv(tsi+tr)-tu(tsj)-it(tsj)v\\ &=(rv-su)jt^2\end{aligned}$$

$$\begin{aligned}(rv-su)i' &\equiv rtu+ritv-sjtv \pmod p\\ &\equiv rtu+ritv-uv\\ &\equiv rtu+ritv-u(tsi+tr)\\ &=(rv-su)it\end{aligned}$$

由于 $(rv-su,p)=1$, 我们有 $j'\equiv jt^2 \pmod p$ 和 $i'\equiv it \pmod p$.

因为 (IVb) 型群的参数 (j,i) 为 $(\nu,0)$, 而 (IVc) 型群的参数 (j',i') 为 $(k,-1)$, 不满足上述条件, 所以 (IVb) 型群和 (IVc) 型群不同构. 容易看出, 当 $i=i'$ 时, 满足上述条件的参数也一定满足 $j'\equiv j \pmod p$, 所以两个不同参数 k 的 (IVc) 型群也互不同构. □

定理 7.1.3. 设 G 是有限亚 *Hamilton* p 群. 若 G' 是 p^2 阶的初等交换群, $c(G)=2$ 且 $d(G)=3$, 则 G 为定理 7.1.2 中的满足 $d(G)=3$ 的群, 即:

(1) $G=\langle a_1,a_2,a_3 \mid a_1^{p^{m_1}}=a_2^{p^{m_2+1}}=a_3^{p^{m_3+1}}=1,[a_1,a_2]=a_3^{p^{m_3}},[a_1,a_3]=a_2^{p^{m_2}},[a_2,a_3]=1\rangle$, 其中 $m_1\geqslant m_2=m_3+1$;

(2) $G=\langle a_1,a_2,a_3 \mid a_1^{p^{m_1}}=a_2^{p^{m_2+1}}=a_3^{p^{m_3+1}}=1,[a_1,a_2]=a_3^{p^{m_3}},[a_1,a_3]=a_2^{\nu p^{m_2}},[a_2,a_3]=1\rangle$, 其中 p 为奇素数, ν 是一个固定的模 p 的平方非剩余, $m_1\geqslant m_2=m_3+1$ 或者 $m_1\geqslant m_2=m_3$;

(3) $G=\langle a_1,a_2,a_3 \mid a_1^{p^{m_1}}=a_2^{p^{m_2+1}}=a_3^{p^{m_3+1}}=1,[a_1,a_2]=a_3^{p^{m_3}},[a_1,a_3]=a_2^{kp^{m_2}}a_3^{-p^{m_3}},[a_2,a_3]=1\rangle$, 其中 $m_1\geqslant m_2=m_3$, 若 p 为奇素数, 则 $1+4k$ 是模 p 的平方非剩余; 若 $p=2$, 则 $k=1$. 满足这种定义关系的群共有 $\frac{p-1}{2}$ 个;

(4) $G=\langle a_1,a_2,a_3 \mid a_1^{p^{m_1+1}}=a_2^{p^{m_2+1}}=a_3^{p^{m_3}}=1,[a_1,a_2]=a_1^{p^{m_1}},[a_1,a_3]=a_2^{p^{m_2}},[a_2,a_3]=1\rangle$, 其中 $m_1\geqslant m_2\geqslant m_3$. 当 $p=2$ 时, $m_1>1$;

(5) $G=\langle a_1,a_2,a_3 \mid a_1^{p^{m_1+1}}=a_2^{p^{m_2}}=a_3^{p^{m_3+1}}=1,[a_1,a_2]=a_3^{p^{m_3}},[a_1,a_3]=a_1^{p^{m_1}},[a_2,a_3]=1\rangle$, 其中 $m_1\geqslant m_2=m_3+1$;

(6) $G = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3}} = 1, [a_1, a_2] = 1, [a_1, a_3] = a_2^{p^{m_2}}, [a_2, a_3] = a_1^{p^{m_1}} \rangle$, 其中 $m_1 - 1 = m_2 \geqslant m_3$;

(7) $G = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3}} = 1, [a_1, a_2] = 1, [a_1, a_3] = a_2^{p^{m_2}}, [a_2, a_3] = a_1^{\nu p^{m_1}} \rangle$, 其中 p 为奇素数, ν 是一个固定的模 p 的平方非剩余, $m_1 - 1 = m_2 \geqslant m_3$ 或 $m_1 = m_2 > m_3$;

(8) $G = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3}} = 1, [a_1, a_2] = 1, [a_1, a_3] = a_2^{p^{m_2}}, [a_2, a_3] = a_1^{kp^{m_1}} a_2^{-p^{m_2}} \rangle$, 其中 $m_1 = m_2 > m_3$, 若 p 为奇素数, 则 $1 + 4k$ 是模 p 的平方非剩余; 若 $p = 2$, 则 $k = 1$. 满足这种定义关系的群共有 $\frac{p-1}{2}$ 个;

(9) $G = \langle a_1, a_2, b \mid a_1^4 = a_2^4 = 1, b^2 = a_1^2, [a_1, a_2] = 1, [a_1, b] = a_2^2, [a_2, b] = a_1^2 \rangle$.

证明　设 G/G' 的型不变量为 $(p^{m_1}, p^{m_2}, p^{m_3})$, 其中 $m_1 \geq m_2 \geqslant m_3$, $G/G' = \langle a_1G' \rangle \times \langle a_2G' \rangle \times \langle a_3G' \rangle$, 其中 $o(a_iG') = p^{m_i}$, $i = 1, 2, 3$. 则 $G = \langle a_1, a_2, a_3 \rangle$.

若 $\langle [a_1, a_3], [a_2, a_3] \rangle = G'$, 设 $[a_1, a_2] = [a_1, a_3]^i [a_2, a_3]^j$. 计算可知

$$[a_1 a_3^j, a_2 a_3^{-i}] = 1.$$

用 $a_1 a_3^j$ 和 $a_2 a_3^{-i}$ 分别去替换 a_1 和 a_2 后, 以上所有关系仍然成立, 因此, 我们可不妨设 $[a_1, a_2] = 1$.

若 $\langle [a_1, a_3], [a_2, a_3] \rangle = \langle [a_2, a_3] \rangle$, 设 $[a_1, a_3] = [a_2, a_3]^i$. 计算可知 $[a_1 a_2^{-i}, a_3] = 1$. 用 $a_1 a_2^{-i}$ 去替换 a_1 后, 以上所有关系仍然成立, 因此, 我们可不妨设 $[a_1, a_3] = 1$. 此时, 必然有 $G' = \langle [a_1, a_2], [a_2, a_3] \rangle$.

若 $\langle [a_1, a_3], [a_2, a_3] \rangle \neq G', \langle [a_2, a_3] \rangle$, 则必然有 $[a_2, a_3] = 1$. 此时,

$$G' = \langle [a_1, a_2], [a_1, a_3] \rangle.$$

设 $G' = \langle x, y \rangle$, 则我们可设 $a_1^{p^{m_1}} = x^i y^j, a_2^{p^{m_2}} = x^s y^t, a_3^{p^{m_3}} = x^u y^v$. 由上可知, 我们只需要考虑以下三种类型的关系:

I. $[a_1, a_2] = x, [a_1, a_3] = y, [a_2, a_3] = 1$;

II. $[a_1, a_2] = 1, [a_1, a_3] = x, [a_2, a_3] = y$;

III. $[a_1, a_2] = x, [a_1, a_3] = 1, [a_2, a_3] = y$;

我们首先考虑 $|G| = p^5$ 的情况. 设 K 是 G 的一个二元生成的非交换群. 由定理 6.1.3 可知 $G' \leqslant K$. 因为 $G' \leqslant Z(G)$, 所以 $G' \leqslant \Phi(K)$. 从而 $|K| \neq p^3$. 这说明 G 的二极大子群都交换. 从而 G 只能是 $\mathcal{A}_2$ 群. 由定理 4.6.1 可知, G 可能是定理中的 (2)、(3)、(4) 型群中 $m_1 = 1$ 的情形, 或者 G 与定理中的 (9) 型群同构. 以下我们设 $|G| > p^5$, 即 $m_1 > 1$.

类型 I: $[a_1, a_2] = x, [a_1, a_3] = y, [a_2, a_3] = 1$.

情形 1: $a_1^{p^{m_1}} = 1$.

由定理 6.1.3 可知 $G' \leqslant \langle a_1, a_3 \rangle$. 所以我们有 $(u, p) = 1$. 分别用 $a_2^u a_3^v$ 和 $x^u y^v$ 去替换 a_2 和 x, 我们可不妨设 $a_3^{p^{m_3}} = x$. 同理 $G' \leqslant \langle a_1, a_2 \rangle$. 所以我们还有 $(t, p) = 1$.

若 $m_2 > m_3$, 我们断言 $p \mid s$. 若否, 考虑子群 $K = \langle a_1, a_2^s a_3^t \rangle$. 计算可知 $[a_1, a_2^s a_3^t] = x^s y^t$, $(a_2^s a_3^t)^{p^{m_2}} = (x^s y^t)^s$, 从而 K 既不交换也不正规, 矛盾. 所以可设 $a_2^{p^{m_2}} = y^t$. 此时再断言 $m_2 - m_3 = 1$. 若否, 考虑子群 $L = \langle a_1, a_2^p a_3 \rangle$. 计算可知 $(a_2^p a_3)^{p^{m_2 - 1}} = y^t = [a_1, a_2^p a_3]^t$. 从而 L 既不交换也不正规, 矛盾. 令 $t^{-1} = \alpha^2 \nu$, 其中 $\nu = 1$ 或者是一个固定的模 p 的平方非剩余. 计算可知 $[a_1^{\alpha^{-1}}, a_2^{\alpha}] = x, [a_1^{\alpha^{-1}}, a_3] = y^{\alpha^{-1}} = a_2^{\alpha^{-1} t^{-1} p^{m_2}} = a_2^{\alpha^{-1} t^{-1} p^{m_2}} = (a_2^{\alpha})^{\nu p^{m_2}}$. 分别用 $a_1^{\alpha^{-1}}$、a_2^{α} 和 $y^{\alpha^{-1}}$ 去替换 a_1、a_2 和 y, 其它关系仍然成立, 因此我们可不妨设 $y = a_2^{\nu p^{m_2}}$. 当 $\nu = 1$, 时, 即得定理中的 (1) 型群; 当 $\nu \neq 1$, 时, 即得定理中的 (2) 型群当 $m_1 \geqslant m_2 = m_3 + 1$ 的情形.

以下我们设 $m_2 = m_3 = m$.

若 $p \mid s$, 令 $t^{-1} = \alpha^2 \nu$, 其中 $\nu = 1$ 或者是一个固定的模 p 的平方非剩余. 计算可知 $[a_1^{\alpha^{-1}}, a_2^{\alpha}] = x, [a_1^{\alpha^{-1}}, a_3] = y^{\alpha^{-1}} = a_2^{\alpha^{-1} t^{-1} p^m} = a_2^{\alpha^{-1} t^{-1} p^m} = (a_2^{\alpha})^{\nu p^m}$. 分别用 $a_1^{\alpha^{-1}}$, a_2^{α} 和 $y^{\alpha^{-1}}$ 去替换 a_1、a_2 和 y, 其它关系仍然成立, 因此我们可不妨设 $y = a_2^{\nu p^m}$. 我们断言 $\nu \neq 1$. 若否, 考虑子群 $K = \langle a_1, a_2 a_3 \rangle$. 计算可知 $[a_1, a_2 a_3] = xy = (a_2 a_3)^{p^m}$, 从而 K 既不交换也不正规, 矛盾. 因此 ν 只能是一个固定的模 p 的平方非剩余, 即得定理中的 (2) 型群当 $m_1 \geqslant m_2 = m_3$ 的情形.

若 $(s, p) = 1$, 令 $a_1' = a_1^{s^{-1} t}, a_3' = a_3^{s^{-1} t}$, $x' = [a_1', a_2] = x^{s^{-1} t}$, $y' = [a_1', a_3'] = y^{s^{-2} t^2}$, $k = s^{-2} t$. 则 $(a_2)^{p^m} = x^s y^t = (x' y')^{k^{-1}}$. 分别用 a_1', a_3' 去替换 a_1, a_3, 我们可不妨设 $[a_1, a_2] = a_3^{p^m}, [a_1, a_3] = a_2^{k p^m} a_3^{-p^m}$. 因为 $(k, p) = 1$,

所以当 $p=2$ 时 $k=1$, 即得定理中的 (3) 型群当 $p=2$ 时的情形. 下面我们证明当 p 为奇素数时一定有 $1+4k$ 是模 p 的平方非剩余. 若否, 设 $1+4k=\beta^2$. 令 $\alpha=2^{-1}k^{-1}(\beta-1)$, 则 $2\alpha k+1\equiv\beta \pmod p$, 从而 $(2\alpha k+1)^2\equiv\beta^2\equiv 1+4k \pmod p$, 化简得 $1-\alpha\equiv\alpha^2k \pmod p$. 我们考虑子群 $L=\langle a_1,a_2a_3^{\alpha}\rangle$. 计算可得 $[a_1,a_2a_3^{\alpha}]=a_3^{p^m}a_2^{\alpha kp^m}a_3^{-\alpha p^m}=a_2^{\alpha kp^m}a_3^{(1-\alpha)p^m}=a_2^{\alpha kp^m}a_3^{\alpha^2kp^m}=(a_2a_3^{\alpha})^{\alpha kp^m}$, 从而 L 既不交换也不正规, 矛盾. 因此我们得定理中的 (3) 型群当 p 为奇素数的情形.

情形 2: $G'=\langle a_1^{p^{m_1}},a_2^{p^{m_2}}\rangle$.

设 $a_3^{p^{m_3}}=a_1^{\alpha p^{m_1}}a_2^{\beta p^{m_2}}$. 计算可知 $(a_3a_1^{-\alpha p^{m_1-m_3}}a_2^{-\beta p^{m_2-m_3}})^{p^{m_3}}=1$. 若 $m_1=m_3$ 且 $(\alpha,p)=1$, 用 $a_3a_1^{-\alpha}a_2^{-\beta}$ 去替换 a_1 后, 可转换为情形 1. 若 $m_1>m_3$ 或 $p\mid\alpha$, 用 $a_3a_1^{-\alpha p^{m_1-m_3}}a_2^{-\beta p^{m_2-m_3}}$ 去替换 a_3 后, 其它关系仍然成立, 因此, 我们可不妨设 $a_3^{p^{m_3}}=1$.

由定理 6.1.3 可知 $G'\leqslant\langle a_1,a_3\rangle$, 所以我们有 $(i,p)=1$. 因为 $[a_1,a_2^ia_3^j]=x^iy^j$, 以 $a_2^ia_3^j$ 和 x^iy^j 替换 a_2 和 x, 我们可不妨设 $a_1^{p^{m_1}}=x$. 此时 $(t,p)=1$.

若 $m_1>m_2$, 计算可知 $(a_2a_1^{-sp^{m_1-m_2}})^{p^{m_2}}=y^t$. 用 $a_2a_1^{-sp^{m_1-m_2}}$, a_3^t 和 y^t 分别去替换 a_2, a_3 和 y, 我们可不妨设 $a_2^{p^{m_2}}=y$. 这就得到了定理中的 (4) 型群.

若 $m_1=m_2$(注意, 此时 $m_1>1$), 我们断言 $p\mid s$, 即 $a_2^{p^{m_2}}=y^t$. 若否, 考虑子群 $K=\langle a_2a_1^{-s},a_3\rangle$. 计算可得 $(a_2a_1^{-s})^{p^{m_2}}=y^t$, $[a_2a_1^{-s},a_3]=y^{-s}$. 从而 K 既不交换也不正规, 矛盾. 用 a_3^t 和 y^t 分别去替换 a_3 和 y, 我们可不妨设 $a_2^{p^{m_2}}=y$. 这就得到了定理中的 (4) 型群.

情形 3: $a_1^{p^{m_1}}\neq 1$ 且 $G'\neq\langle a_1^{p^{m_1}},a_2^{p^{m_2}}\rangle$.

考虑子群 $K=\langle a_1,a_2^ia_3^j\rangle$. 因为 $[a_1,a_2^ia_3^j]=x^iy^j=a_1^{p^{m_1}}\neq 1$, 所以 $K\trianglelefteq G$, 从而由定理 6.1.3 可得 $G'\leqslant K$. 因为 $a_2^{p^{m_2}}\in\langle a_1^{p^{m_1}}\rangle$, 所以 $(j,p)=1$, 且 $G'=\langle a_1^{p^{m_1}},a_3^{p^{m_3}}\rangle$. 此时, 若 $m_2=m_3$, 互换 a_2 与 a_3 后可转化为情形 2. 因此, 我们可不妨设 $m_2>m_3$. 此时, 进一步考虑子群 K 有 $p\mid i$, 即 $a_1^{p^{m_1}}=y^j$.

计算可知 $(a_3a_1^{-j^{-1}rp^{m_1-m_3}})^{p^{m_3}}=x^u$. 以 $a_3a_2^{-j^{-1}rp^{m_1-m_3}}$ 替换 a_3 后, 其它关系不变. 因此, 可不妨设 $a_3^{p^{m_3}}=x^u$. 显然, $(u,p)=1$.

因为 $a_2^{p^{m_2}}\in\langle a_1^{p^{m_1}}\rangle$, 所以可设 $a_2^{p^{m_2}}=a_1^{rp^{m_1}}$. 若 $(r,p)=1$ 且 $m_1=m_2$, 用 $a_2a_1^{-r}$ 替换 a_1, 可以转化为情形 1; 若 $m_1>m_2$ 或 $p\mid r$, 用 $a_2a_1^{-rp^{m_1-m_2}}$ 替

换 a_2, 我们可不妨设 $a_2^{p^{m_2}}=1$.

断言 $m_2-m_3=1$. 若否, $m_2-1>m_3$ 考虑子群 $J=\langle a_1, a_2^pa_3\rangle$. J 既不交换也不正规, 矛盾.

分别用 a_2^{ju}, x^{ju}, a_3^j 和 y^j 替换 a_2, x, a_3 和 y 我们可不妨设 $a_1^{p^{m_1}}=y$, $a_3^{p^{m_3}}=x$. 即得定理中的 (5) 型群.

类型 II: $[a_1,a_2]=1, [a_1,a_3]=x, [a_2,a_3]=y$.

若 $m_1=m_3$, 可转换为类型 I. 因此, 我们可设 $m_1>m_3$.

情形 1: $m_1>m_2$.

首先我们断言 $p\mid i$(即 $a_1^{p^{m_1}}=y^j$). 若否, 则 $(i,p)=1$. 考虑子群

$$J=\langle a_2^ia_1^{-sp^{m_1-m_2}}, a_3^ia_1^{-up^{m_1-m_3}}\rangle.$$

计算得

$$[a_2^ia_1^{-sp^{m_1-m_2}}, a_3^ia_1^{-up^{m_1-m_3}}]=y^{i^2}\neq 1,$$

$(a_2^ia_1^{-sp^{m_1-m_2}})^{p^{m_2}}=y^{ti-sj}, (a_3^ia_1^{-up^{m_1-m_3}})^{p^{m_3}}=y^{vi-uj}$. 从而 J 既不交换也不正规, 矛盾.

接着我们断言 $a_1^{p^{m_1}}\neq 1$(即 $(j,p)=1$). 若否, 考虑子群 $K=\langle a_1^ua_2^v, a_3\rangle$. 计算得 $[a_1^ua_2^v, a_3]=x^uy^v=a_3^{p^{m_3}}$. 若 $(u,p)=1$, 则 K 既不交换也不正规. 所以一定有 $a_3^{p^{m_3}}=y^v$. 再考虑子群 $L=\langle a_2,a_3\rangle$. 由于 $G'=\langle x,y\rangle\leqslant L$, 所以有 $(s,p)=1$. 最后分三种情况导出最后的矛盾. (1) 当 $m_2>m_3$ 时, 考虑子群 $M=\langle a_1a_3^{-t}, a_2a_3^s\rangle$. 计算可得 $[a_1a_3^{-t}, a_2a_3^s]=x^sy^t=(a_2a_3^s)^{p^{m_2}}\neq 1$, 可知 M 既不交换也不正规, 矛盾. (2) 当 $m_2=m_3>1$ 或 $m_2=1$ 但 p 为奇素数时, 考虑子群 $N=\langle a_1^sa_2^{t+v}, a_2a_3\rangle$. 计算得 $[a_1^sa_2^{t+v}, a_2a_3]=x^sy^{t+v}=(a_2a_3)^{p^{m_3}}$, 可知 N 既不交换也不正规, 矛盾. (3) 当 $m_2=1$ 且 $p=2$ 时, 考虑子群 $O=\langle a_1^sa_2^{t+v+1}, a_2a_3\rangle$. 计算得 $[a_1^sa_2^{t+v+1}, a_2a_3]=x^sy^{t+v+1}=(a_2a_3)^2$, 可知 O 既不交换也不正规, 矛盾.

计算可得

$$(a_2a_1^{-j^{-1}tp^{m_1-m_2}})^{p^{m_2}}=x^sy^t(x^iy^j)^{-j^{-1}t}=x^{s-j^{-1}it},$$

$$(a_3a_1^{-j^{-1}vp^{m_1-m_3}})^{p^{m_3}}=x^uy^v(x^iy^j)^{-j^{-1}v}=x^{u-j^{-1}iv}.$$

分别用 $a_2a_1^{-j^{-1}tp^{m_1-m_2}}$ 和 $a_3a_1^{-j^{-1}vp^{m_1-m_3}}$ 去替换 a_2 和 a_3, 其它关系仍然成立, 因此我们可不妨设 $a_2^{p^{m_2}}=x^s, a_3^{p^{m_3}}=x^u$.

我们断言 $(s,p)=1$. 若否, 则 $a_2^{p^{m_2}}=1$. 首先考虑子群 $P=\langle a_2, a_1a_3\rangle$, 因为 $[a_2, a_1a_3]=y\neq 1$, 所以 $P\trianglelefteq G$. 由定理 6.1.3 可得 $G'\leqslant P$, 从而 $(i,p)=1$. 再考虑子群 $Q=\langle a_2, a_3^ia_1^{-up^{m_1-m_3}}\rangle$. 计算可得 $[a_2, a_3^ia_1^{-up^{m_1-m_3}}]=y^i\neq 1$, $(a_3^ia_1^{-up^{m_1-m_3}})^{p^{m_3}}=x^{iu}(x^iy^j)^{-u}=y^{-ju}$, 从而 Q 既不交换也不正规, 矛盾.

因为 $a_2^{p^{m_2}}=x^s=[a_1^s, a_3]$, 用 a_1^s 和 x^s 去替换 a_1 和 x, 其它关系不变, 所以, 我们可设 $a_2^{p^{m_2}}=x$.

若 $m_2>1$ 或 p 为奇素数, 计算可得

$$(a_3a_2^{-up^{m_2-m_3}})^{p^{m_3}}=x^ux^{-u}=1.$$

用 $a_3a_2^{-up^{m_2-m_3}}$ 去替换 a_3, 其它关系仍然成立, 此时我们可不妨设 $a_3^{p^{m_3}}=1$. 若 $m_2=1$ 且 $p=2$, 计算可得 $(a_3a_2^ua_1^{u2^{m_1-1}})^2=x^ux^uy^uy^u=1$. 用 $a_3a_2^ua_1^{u2^{m_1-1}}$ 去替换 a_3, 其它关系仍然成立, 此时我们仍可不妨设 $a_3^{p^{m_3}}=1$.

进一步, 我们断言 $m_1-m_2=1$. 若否, 考虑子群 $R=\langle a_2a_1^{p^{m_1-m_2-1}}, a_3\rangle$. 注意到 $(a_2a_1^{p^{m_1-m_2-1}})^{p^{m_2+1}}=a_1^{p^{m_1}}=y^j=[a_2a_1^{p^{m_1-m_2-1}}, a_3]^j$, 可得出 R 既不交换也不正规, 矛盾. 因此, $m_2=m_1-1$.

令 $j^{-1}=\alpha^2\nu$, 其中 $\nu=1$ 或者是一个固定的模 p 的平方非剩余. 计算可知 $[a_2, a_3^{\alpha^{-1}}]=y^{\alpha^{-1}}=a_1^{j^{-1}\alpha^{-1}p^{m_1}}=a_1^{\alpha\nu p^{m_1}}=(a_1^{\alpha})^{\nu p^{m_1}}$. 分别用 a_1^{α}, $a_3^{\alpha^{-1}}$ 和 $y^{\alpha^{-1}}$ 去替换 a_1, a_3 和 y, 其它关系仍然成立, 因此我们可不妨设 $y=a_1^{\nu p^{m_1}}$. 当 $\nu=1$, 时, 即得定理中的 (6) 型群; 当 $\nu\neq 1$, 时, 即得定理中的 (7) 型群当 $m_1-1=m_2\geqslant m_3$ 的情况.

情形 2. $m_1=m_2=m>m_3$.

首先我们断言 $a_1^{p^{m_1}}=x^iy^j\neq 1$. 若否, 因为 $[a_1a_3^{-t}, a_2a_3^s]=x^sy^t=(a_2a_3^s)^{p^{m_2}}$, 所以 $M=\langle a_1a_3^{-t}, a_2a_3^s\rangle \ntrianglelefteq G$, 因而 M 交换, $a_2^{p^{m_2}}=x^sy^t=1$. 但这时, $\langle a_1, a_2a_3\rangle$ 既不交换也不正规, 矛盾.

接下来我们断言 $G'=\langle a_1^{p^{m_1}}, a_2^{p^{m_2}}\rangle$. 令 $M=\langle a_1a_3^{-j}, a_2a_3^i\rangle$, 因为

$$[a_1a_3^{-j}, a_2a_3^i]=x^iy^j=(a_1a_3^{-t})^{p^{m_1}}\neq 1,$$

所以 $M\trianglelefteq G$. 从而由定理 6.1.3 可得 $G'\leqslant M$. 所以我们有 $a_2^{p^{m_2}}\notin\langle x^iy^j\rangle$, $G'=\langle a_1^{p^{m_1}}, a_2^{p^{m_2}}\rangle$.

设 $a_3^{p^{m_3}}=a_1^{\alpha p^{m_1}}a_2^{\beta p^{m_2}}$. 计算可知 $(a_3a_1^{-\alpha p^{m_1-m_3}}a_2^{-\beta p^{m_2-m_3}})^{p^{m_3}}=1$. 用

$$a_3a_1^{-\alpha p^{m_1-m_3}}a_2^{-\beta p^{m_2-m_3}}$$

去替换 a_3 后, 其它关系仍然成立, 因此, 我们可不妨设 $a_3^{p^{m_3}}=1$.

因为 $G'\leqslant\langle a_2,a_3\rangle$, 我们有 $(s,p)=1$. 由于 $[a_1^sa_2^t,a_3]=x^sy^t$, 分别用 $a_1^sa_2^t$ 和 x^sy^t 去替换 a_1 和 x. 其它关系仍然成立, 因此我们可不妨设 $a_2^{p^{m_2}}=x$.

因为 $G'\leqslant\langle a_1,a_3\rangle$, 我们有 $(j,p)=1$.

若 $p\mid i$(即 $a_1^{p^{m_1}}=y^j$). 令 $j^{-1}=\alpha^2\nu$, 其中 $\nu=1$ 或者是一个固定的模 p 的平方非剩余. 计算可知 $[a_2,a_3^{\alpha^{-1}}]=y^{\alpha^{-1}}=a_1^{j^{-1}\alpha^{-1}p^{m_1}}=a_1^{\alpha\nu p^{m_1}}=(a_1^{\alpha})^{\nu p^{m_1}}$. 分别用 a_1^{α}, $a_3^{\alpha^{-1}}$ 和 $y^{\alpha^{-1}}$ 去替换 a_1, a_3 和 y, 其它关系仍然成立, 因此我们可不妨设 $y=a_1^{\nu p^{m_1}}$. 我们断言 $\nu\neq1$. 若否, 考虑子群 $K=\langle a_1a_2,a_3\rangle$. 因为 $[a_1a_2,a_3]=xy=(a_1a_2)^{p^{m_1}}$, 所以 K 既不交换也不正规, 矛盾. 从而 ν 只能是一个固定的模 p 的平方非剩余. 显然, 此时 p 为奇素数, 即得定理中的 (7) 型群当 $m_1=m_2>m_3$ 的情况.

若 $(i,p)=1$, 令 $a_1'=a_2^i,a_2'=a_1a_2^{-i},a_3=a_3^{ji^{-1}}$, $x'=[a_1',a_3']=y^j$, $y'=[a_2',a_3']=x^{ji^{-1}}y^{-j}$, $k=ji^{-2}$, 则 $(a_2')^{p^m}=x^iy^jx^{-i}=y^j=x'$, $(a_1')^{p^m}=x^i=(x'y')^{j^{-1}i^2}=(x'y')^{k^{-1}}$. 分别用 a_1',a_2',a_3' 去替换 a_1,a_2,a_3, 我们不妨设 $[a_1,a_2]=1,[a_1,a_3]=x=a_2^{p^m},[a_2,a_3]=y=a_1^{kp^m}a_2^{-p^m}$. 当 $p=2$ 时, k 只能取 1, 从而得到定理中的 (8) 型群当 $p=2$ 时的情况. 下面我们证明当 p 为奇素数时一定有 $1+4k$ 是模 p 的平方非剩余. 若否, 设 $1+4k=\beta^2$. 令 $\alpha=2^{-1}k^{-1}(\beta-1)$, 则 $2\alpha k+1\equiv\beta\pmod p$, 从而 $(2\alpha k+1)^2\equiv\beta^2\equiv1+4k\pmod p$, 化简得 $1-\alpha\equiv\alpha^2k\pmod p$. 我们考虑子群 $L=\langle a_1a_2^{\alpha},a_3\rangle$. 计算可得 $[a_1a_2^{\alpha},a_3]=a_2^{p^m}a_1^{\alpha kp^m}a_2^{-\alpha p^m}=a_1^{\alpha kp^m}a_2^{(1-\alpha)p^m}=a_1^{\alpha kp^m}a_2^{\alpha^2kp^m}=(a_1a_2^{\alpha})^{\alpha kp^m}$, 从而 L 既不交换也不正规, 矛盾. 因此我们得定理中的 (8) 型群当 p 为奇素数的情形.

类型 III: $[a_1,a_2]=x,[a_1,a_3]=1,[a_2,a_3]=y$.

我们要证明, 这种情况下得不到新的群. 此时, 若 $m_2=m_3$, 互换 a_2 与 a_3 后可转化为类型 II; 若 $m_1=m_2$, 互换 a_1 与 a_2 后可转化为类型 I. 因此, 若假设有新的群存在, 则一定有 $m_1>m_2>m_3$.

首先我们断言 $a_1^{p^{m_1}}=y^j$. 若否, 则 $(i,p)=1$. 考虑子群

$$J=\langle a_2^ia_1^{-sp^{m_1-m_2}},a_3^ia_1^{-up^{m_1-m_3}}\rangle.$$

计算得

$$[a_2^i a_1^{-sp^{m_1-m_2}}, a_3^i a_1^{-up^{m_1-m_3}}] = y^{i^2} \neq 1,$$

$$(a_2^i a_1^{-sp^{m_1-m_2}})^{p^{m_2}} = y^{ti-sj}, (a_3^i a_1^{-up^{m_1-m_3}})^{p^{m_3}} = y^{vi-uj}.$$

从而 J 既不交换也不正规, 矛盾.

断言 $(s,p)=1$. 若否, 则 $a_2^{p^{m_2}} = y^t$. 考虑子群 $K = \langle a_2, a_3 a_1^p \rangle$. 计算得 $[a_2, a_3 a_1^p] = y \neq 1$, $(a_3 a_1^p)^{p^{m_1-1}} = a_1^{p^{m_1}} = y^j$, 从而 K 既不交换也不正规, 矛盾.

断言 $a_1^{p^{m_1}} \neq 1$, 即 $(j,p)=1$. 若否, 考虑子群 $L = \langle a_2, a_1^{-s} a_3 \rangle$. 计算得, $[a_2, a_1^{-s} a_3] = x^s y^t = a_2^{p^{m_2}} \neq 1$, $(a_1^{-s} a_3)^{p^{m_1}} = 1$, 从而 L 既不交换也不正规, 矛盾.

最后, 考虑子群 $M = \langle a_1 a_2, a_3^s a_2^{-up^{m_2-m_3}} \rangle$. 计算得, $[a_1 a_2, a_3^s a_2^{-up^{m_2-m_3}}] = y^s \neq 1$, $(a_1 a_2)^{p^{m_1}} = y^j$, $(a_3^s a_2^{-up^{m_2-m_3}})^{p^{m_3}} = y^{sv-tu}$. 从而 L 既不交换也不正规, 矛盾. □

定理 7.1.4. *设 G 是有限亚 Hamilton p 群, G' 为 p^2 阶初等交换群且 $c(G)=2$, 则 G 为定理 7.1.2 中的群, 即:*

(1) *$G = K \times A$. 其中 $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3+1}} = 1, [a_1,a_2] = a_3^{p^{m_3}}, [a_1,a_3] = a_2^{p^{m_2}}, [a_2,a_3]=1 \rangle$, $m_1 \geqslant m_2 = m_3+1$, A 是满足 $\exp(A) \leqslant p^{m_3}$ 的交换群;*

(2) *$G = K \times A$. 其中 $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3+1}} = 1, [a_1,a_2] = a_3^{p^{m_3}}, [a_1,a_3] = a_2^{\nu p^{m_2}}, [a_2,a_3]=1 \rangle$, 其中 p 为奇素数, ν 是一个固定的模 p 的平方非剩余, $m_1 \geqslant m_2 = m_3+1$ 或者 $m_1 \geqslant m_2 = m_3$. A 是满足 $\exp(A) \leqslant p^{m_3}$ 的交换群;*

(3) *$G = K \times A$. 其中 $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3+1}} = 1, [a_1,a_2] = a_3^{p^{m_3}}, [a_1,a_3] = a_2^{kp^{m_2}} a_3^{-p^{m_3}}, [a_2,a_3]=1 \rangle$, 其中 $m_1 \geqslant m_2 = m_3$. 若 p 为奇素数, 则 $1+4k$ 是模 p 的平方非剩余; 若 $p=2$, 则 $k=1$. A 是满足 $\exp(A) \leqslant p^{m_3}$ 的交换群;*

(4) *$G = K \times A$. 其中 $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3}} = 1, [a_1,a_2] = a_1^{p^{m_1}}, [a_1,a_3] = a_2^{p^{m_2}}, [a_2,a_3]=1 \rangle$, 其中 $m_1 \geqslant m_2 \geqslant m_3$. A 是满足 $\exp(A) \leqslant p^{m_2}$ 的交换群;*

(5) $G=K\times A$. 其中 $K=\langle a_1,a_2,a_3\mid a_1^{p^{m_1+1}}=a_2^{p^{m_2}}=a_3^{p^{m_3+1}}=1,[a_1,a_2]=a_3^{p^{m_3}},[a_1,a_3]=a_1^{p^{m_1}},[a_2,a_3]=1\rangle$, 其中 $m_1\geqslant m_2=m_3+1$. A 是满足 $\exp(A)\leqslant p^{m_3}$ 的交换群;

(6) $G=K\times A$. 其中 $K=\langle a_1,a_2,a_3\mid a_1^{p^{m_1+1}}=a_2^{p^{m_2+1}}=a_3^{p^{m_3}}=1,[a_1,a_2]=1,[a_1,a_3]=a_2^{p^{m_2}},[a_2,a_3]=a_1^{p^{m_1}}\rangle$, 其中 $m_1-1=m_2\geqslant m_3$. A 是满足 $\exp(A)\leqslant p^{m_2}$ 的交换群;

(7) $G=K\times A$. 其中 $K=\langle a_1,a_2,a_3\mid a_1^{p^{m_1+1}}=a_2^{p^{m_2+1}}=a_3^{p^{m_3}}=1,[a_1,a_2]=1,[a_1,a_3]=a_2^{p^{m_2}},[a_2,a_3]=a_1^{\nu p^{m_1}}\rangle$, 其中 p 为奇素数, ν 是一个固定的模 p 的平方非剩余, $m_1-1=m_2\geqslant m_3$ 或者 $m_1=m_2>m_3$, A 是满足 $\exp(A)\leqslant p^{m_2}$ 的交换群;

(8) $G=K\times A$. 其中 $K=\langle a_1,a_2,a_3\mid a_1^{p^{m_1+1}}=a_2^{p^{m_2+1}}=a_3^{p^{m_3}}=1,[a_1,a_2]=1,[a_1,a_3]=a_2^{p^{m_2}},[a_2,a_3]=a_1^{kp^{m_1}}a_2^{-p^{m_2}}\rangle$, 其中 $m_1=m_2>m_3$, 若 p 为奇素数, 则 $1+4k$ 是模 p 的平方非剩余; 若 $p=2$, 则 $k=1$. A 是满足 $\exp(A)\leqslant p^{m_2}$ 的交换群;

(9) $G=K\times A$. 其中 $K=\langle a_1,a_2,b\mid a_1^4=a_2^4=1,b^2=a_1^2,[a_1,a_2]=1,[a_1,b]=a_2^2,[a_2,b]=a_1^2\rangle$, A 是满足 $\exp(A)\leqslant 2$ 的交换群;

(10) $G=K\times A$. 其中 $K=\langle a_1,a_2,b,d\mid a_1^4=a_2^4=1,b^2=a_1^2,d^2=a_2^2,[a_1,a_2]=1,[a_1,b]=a_2^2,[a_2,b]=a_1^2,[a_1,d]=a_1^2,[a_2,d]=a_1^2a_2^2,[b,d]=1\rangle$, A 是满足 $\exp(A)\leqslant 2$ 的交换群.

证明 设 G/G' 的型不变量为 $(p^{m_1},p^{m_2},\ldots,p^{m_r})$, 其中 $m_1\geqslant m_2\geq\cdots\geqslant m_r$, $G/G'=\langle a_1G'\rangle\times\langle a_2G'\rangle\times\cdots\times\langle a_rG'\rangle$, 其中 $o(a_iG')=p^{m_i}$, $i=1,2,\ldots,r$. 则 $G=\langle a_1,a_2,\ldots,a_r\rangle$.

若 $m_1=1$, 则 G/G' 为初等交换 p 群. 任取 G 的两个非交换的元素 x,y, 由定理 6.1.3 可知, $G'\leqslant\langle x,y\rangle$, 从而 $\langle x,y\rangle$ 为 p^4 阶的内交换群. 这说明 G 是 $\mathcal{T}_4$ 群, 从而 G 是定理 5.2.6 中的群. 它们分别与定理中的 (9) 型群, (10) 型群, 以及 (4) 型群, (2) 型群, (3) 型群中 $m_1=m_2=m_3=1$ 的情形相对应. 以下设 $m_1>1$.

设 i 是使 a_i 不在 $Z(G)$ 中的最小的正整数, 即存在 $j>i$ 使 $[a_i,a_j]\neq 1$. 若 $i\neq 1$, 说明 a_1 在 $Z(G)$ 中, 从而 $[a_1a_j,a_i]\neq 1$, 此时, 我们可以用 a_1a_j 来替换 a_1, 仍然有其它的关系成立. 所以, 我们可不妨设 $i=1$, 即 $a_1\notin Z(G)$.

再设 j 是使 $[a_1,a_j]\neq 1$ 的最小的正整数. 若 $j\neq 2$, 说明 $[a_1,a_2]=1$, 从而 $[a_1,a_2a_j]\neq 1$, 此时, 我们可以用 a_2a_j 来替换 a_2, 仍然有上面的关系成立. 所以, 我们可不妨设 $j=2$, 即 $[a_1,a_2]\neq 1$.

再设 k 是使 $[a_k,a_l]\notin\langle[a_1,a_2]\rangle$ 的最小正整数. 若 $k>2$, 说明对所有的 s 都有 $[a_1,a_s]\in\langle[a_1,a_2]\rangle, [a_2,a_s]\in\langle[a_1,a_2]\rangle$. (1) 如果 $[a_1,a_l]=1$, 我们有 $[a_1,a_2a_l]=[a_1,a_2], [a_2a_l,a_k]=[a_2,a_k][a_l,a_k]\notin\langle[a_1,a_2]\rangle$. 此时, 我们用 a_2a_l 来替换 a_2, 仍然有其它的关系成立. 所以, 我们可不妨设 $k\leqslant 2$. (2) 如果 $[a_1,a_l]=[a_1,a_2]^{\alpha}$, 其中 $(\alpha,p)=1$, 再设 $[a_1,a_k]=[a_1,a_2]^{\beta}$, 我们有 $[a_1,a_ka_l^{\alpha^{-1}\beta}]=1$, $[a_1,a_2a_ka_l^{\alpha^{-1}\beta}]=[a_1,a_2]$, $[a_2a_ka_l^{\alpha^{-1}\beta},a_l]=[a_2,a_l][a_k,a_l]\notin\langle[a_1,a_2]\rangle$. 此时, 我们用 $a_2a_ka_l^{\alpha^{-1}\beta}$ 来替换 a_2, 仍然有其它的关系成立. 所以, 我们可不妨设 $k\leqslant 2$.

再设 l 是使 $[a_k,a_l]\notin\langle[a_1,a_2]\rangle$ 的最小正整数. 若 $l\neq 3$, 说明 $[a_1,a_3]\in\langle[a_1,a_2]\rangle$, $[a_2,a_3]\in\langle[a_1,a_2]\rangle$, 从而 $[a_k,a_3a_l]=[a_k,a_3][a_k,a_l]\notin\langle[a_1,a_2]\rangle$, 此时, 我们用 a_3a_l 来替换 a_3, 仍然有其它的关系成立. 所以, 我们可不妨设 $l=3$.

令 $K=\langle a_1,a_2,a_3\rangle$, 则 $|K'|=|G'|=p^2$ 且 $d(K)=3$, 从而 K 与定理 7.1.3 中的群之一同构. 若 $r=3$, K 已经是群 G. 下面我们设 $r\geqslant 4$ 并逐一进行讨论:

情形 1: K 与定理 7.1.3 中的 (1) 型群同构.

设 $a_4^{p^{m_4}}=a_2^{\alpha p^{m_2}}a_3^{\beta p^{m_3}}$. (1): 若 $m_3>1$ 或者 p 为奇素数, 则

$$(a_4a_2^{-\alpha p^{m_2-m_4}}a_3^{-\beta p^{m_3-m_4}})^{p^{m_4}}=1,$$

我们用 $a_4a_2^{-\alpha p^{m_2-m_4}}a_3^{-\beta p^{m_3-m_4}}$ 来替换 a_4, 仍然有其它的关系成立. 所以, 我们可不妨设 $a_4^{p^{m_4}}=1$. (2): 若 $m_3=1$ 且 $p=2$, 则 $m_2=2$, $(a_4a_2^{-2\alpha}a_3^{-\beta})^2=[a_3,a_4]^{\beta}$. (i) 若 $[a_3,a_4]^{\beta}=1$, 我们用 $a_4a_2^{-2\alpha}a_3^{-\beta}$ 来替换 a_4, 仍然有其它的关系成立. 所以, 我们可不妨设 $a_4^2=1$. (ii) 若 $[a_3,a_4]^{\beta}\neq 1$, 则 $(a_4a_2^{-2\alpha})^2=a_3^2$. 考虑子群 $L=\langle a_4a_2^{-2\alpha},a_3\rangle$. 因为 $[a_4a_2^{-2\alpha},a_3]=[a_4,a_3]\neq 1$, 所以 $L\trianglelefteq G$, 从而 $a_2^4=[a_1,a_3]\in L$. 所以我们可设 $[a_3,a_4]=a_2^4a_3^{2\gamma}$. 再考虑子群 $M=\langle a_1a_4,a_3\rangle$, 若 $[a_1a_4,a_3]=a_3^{2\gamma}\neq 1$, 则 M 既不交换也不正规, 所以我们一定有 $[a_3,a_4]=a_2^4$. 计算可得 $(a_4a_2^{2(1-\alpha)}a_3)^2=a_4^2a_2^{4-4\alpha}a_3^2[a_3,a_4]=1$. 我们用 $a_4a_2^{2(1-\alpha)}a_3$ 来替换 a_4, 仍然有其它的关系成立. 所以, 我们可不妨设 $a_4^2=1$.

由上面我们知道, 可以不妨设 $a_4^{p^{m_4}}=1$. 考虑子群 $N=\langle a_1a_3^i,a_4\rangle$, 若 $[a_1a_3^i,a_4]\neq 1$, 则 N 既不交换也不正规, 所以一定有 $[a_1,a_4]=1$, $[a_3,a_4]=1$.

我们断言 $[a_2,a_4]=1$. 若否, 考虑子群 $O=\langle a_2,a_4\rangle$, 因为 O 非交换, 所以 $O\trianglelefteq G$, 从而由定理 6.1.3 得 $a_3^{p^{m_3}}\in O$. 此时, 我们可设 $[a_2,a_4]=a_2^{\alpha p^{m_2}}a_3^{\beta p^{m_3}}$, 其中 $(\beta,p)=1$. 再考虑子群 $P=\langle a_1^{\beta}a_4,a_2a_3^{\beta^{-1}(\alpha+1)}\rangle$, 计算可得

$$\begin{aligned}[a_1^{\beta}a_4,a_2a_3^{\beta^{-1}(\alpha+1)}] &= [a_1,a_2]^{\beta}[a_1,a_3]^{\alpha+1}[a_4,a_2]\\ &= a_3^{\beta p^{m_3}}a_2^{(\alpha+1)p^{m_2}}a_2^{-\alpha p^{m_2}}a_3^{-\beta p^{m_3}}\\ &= a_2^{p^{m_2}}=(a_2a_3^{\beta^{-1}(\alpha+1)})^{p^{m_2}}\end{aligned}$$

所以 P 既不交换也不正规, 矛盾.

同理, 我们可不妨设 $a_i^{p^{m_i}}=1$, 其中 $i=5,6,\ldots,r$. 并且, 同理可证明 $[a_1,a_i]=[a_2,a_i]=[a_3,a_i]=1$.

若 $r\geqslant 5$, 同理我们还可以证明 $[a_i,a_j]=1$, 其中 $4\leqslant i<j\leq r$. 这种情形下, $G\cong K\times A$, 其中 A 是满足 $\exp(A)\leqslant p^{m_3}$ 的交换群. 从而我们得到了定理中的 (1) 型群.

情形 2: K 与定理 7.1.3 中的 (2) 型群同构.

设 $a_4^{p^{m_4}}=a_2^{\alpha p^{m_2}}a_3^{\beta p^{m_3}}$, 则

$$(a_4a_2^{-\alpha p^{m_2-m_4}}a_3^{-\beta p^{m_3-m_4}})^{p^{m_4}}=1.$$

我们用 $a_4a_2^{-\alpha p^{m_2-m_4}}a_3^{-\beta p^{m_3-m_4}}$ 来替换 a_4, 仍然有其它的关系成立. 所以, 我们可不妨设 $a_4^{p^{m_4}}=1$. 考虑子群 $L=\langle a_1,a_4\rangle$, 若 $[a_1,a_4]\neq 1$, 则 L 既不交换也不正规, 所以一定有 $[a_1,a_4]=1$. 下面我们分两种情况讨论.

(1) $m_2=m_3+1$.

考虑子群 $M=\langle a_1a_3,a_4\rangle$, 若 $[a_1a_3,a_4]\neq 1$, 则 M 既不交换也不正规, 所以一定有 $[a_1a_3,a_4]=1$, 从而 $[a_3,a_4]=1$. 我们断言 $[a_2,a_4]=1$. 若否, 考虑子群 $N=\langle a_2,a_4\rangle$, 因为 N 非交换, 所以 $N\trianglelefteq G$, 从而由定理 6.1.3 得 $a_3^{p^{m_3}}\in N$. 此时, 我们可设 $[a_2,a_4]=a_2^{\alpha p^{m_2}}a_3^{\beta p^{m_3}}$, 其中 $(\beta,p)=1$. 再考虑子群 $O=\langle a_1^{\beta}a_4,a_2a_3^{\beta^{-1}\nu^{-1}(\alpha+1)}\rangle$, 计算可得

$$\begin{aligned}[a_1^{\beta}a_4,a_2a_3^{\beta^{-1}\nu^{-1}(\alpha+1)}] &= [a_1,a_2]^{\beta}[a_1,a_3]^{\nu^{-1}(\alpha+1)}[a_4,a_2]\\ &= a_3^{\beta p^{m_3}}a_2^{(\alpha+1)p^{m_2}}a_2^{-\alpha p^{m_2}}a_3^{-\beta p^{m_3}}\\ &= a_2^{p^{m_2}}=(a_2a_3^{\beta^{-1}\nu^{-1}(\alpha+1)})^{p^{m_2}}\end{aligned}$$

所以 O 既不交换也不正规, 矛盾.

同理, 我们可不妨设 $a_i^{p^{m_1}} = 1$, 其中 $i = 5, 6, \ldots, r$. 并且, 同理可证明 $[a_1, a_i] = [a_2, a_i] = [a_3, a_i] = 1$.

若 $r \geqslant 5$, 我们还可以证明 $[a_i, a_j] = 1$, 其中 $4 \leqslant i < j \leqslant r$. 这种情形下, $G \cong K \times A$, 其中 A 是满足 $\exp(A) \leqslant p^{m_3}$ 的交换群. 从而我们得到了定理中的 (2) 型群当 $m_1 \geqslant m_2 = m_3 + 1$ 的情形.

(2) $m_2 = m_3$.

首先我们断言 $[a_3, a_4] \in \langle a_2^{p^{m_2}} \rangle$. 若否, 设 $[a_3, a_4] = a_2^{\alpha p^{m_2}} a_3^{\gamma p^{m_3}}$, 其中 $(\gamma, p) = 1$. 则子群 $M = \langle a_3, a_4 a_1^{\alpha\nu^{-1}} \rangle$, 既不交换也不正规, 矛盾. 所以一定有 $[a_3, a_4] = a_2^{\alpha p^{m_2}}$.

我们断言 $[a_2, a_4] \in \langle a_3^{p^{m_3}} \rangle$. 若否, 设 $[a_2, a_4] = a_2^{\gamma p^{m_2}} a_3^{\beta p^{m_3}}$, 其中 $(\gamma, p) = 1$. 则子群 $N = \langle a_2, a_4 a_1^{\beta} \rangle$ 既不交换也不正规, 矛盾. 所以一定有 $[a_2, a_4] = a_3^{\beta p^{m_3}}$.

令 $\delta = (\nu - 1)^{-1}(\alpha - \beta)$, 则 $\delta\nu - \alpha = \delta - \beta$. 计算可得

$$
\begin{aligned}
[a_2 a_3, a_4 a_1^{\delta}] &= [a_2, a_4][a_2, a_1]^{\delta}[a_3, a_4][a_3, a_1]^{\delta} \\
&= a_3^{\beta p^{m_3}} a_3^{-\delta p^{m_3}} a_2^{\alpha p^{m_2}} a_2^{-\delta\nu p^{m_2}} \\
&= a_2^{(\alpha - \delta\nu) p^{m_2}} a_3^{(\beta - \delta) p^{m_3}} \\
&= (a_2 a_3)^{(\beta - \delta) p^{m_2}}
\end{aligned}
$$

若 $(a_2 a_3)^{(\beta - \delta) p^{m_2}} \neq 1$, 则子群 $\langle a_2 a_3, a_4 a_1^{\delta} \rangle$ 既不交换也不正规, 所以一定有

$$(a_2 a_3)^{(\beta - \delta) p^{m_2}} = 1.$$

即 $\beta = \delta$, 由此可得 $\alpha = \beta\nu$. 若 $(\beta, p) = 1$, 用 $a_4^{-\beta^{-1}}$ 替换 a_4, 我们可不妨设 $[a_4, a_2] = a_3^{p^{m_3}}$, $[a_4, a_3] = a_2^{\nu p^{m_2}}$. 若 $m_1 = m_4$, 再用 $a_4 a_1^{-1}$ 替换 a_4, 我们可不妨 $[a_1, a_4] = [a_2, a_4] = [a_3, a_4] = 1$

同理, 我们可不妨设 $a_i^{p^{m_1}} = 1$, 其中 $i = 5, 6, \ldots, r$. 并且, 同理可不妨设 $[a_1, a_i] = [a_2, a_i] = [a_3, a_i] = 1$, 或者当 $m_1 > m_i$ 时设 $[a_i, a_1] = 1$, $[a_i, a_2] = a_3^{p^{m_3}}$, $[a_i, a_3] = a_2^{\nu p^{m_2}}$.

若 $r \geqslant 5$, 我们还可以断言 $[a_i, a_j] = 1$, 其中 $4 \leqslant i < j \leqslant r$. 若否, 则 $[a_1 a_i, a_j] \neq 1$. 此时, 子群 $\langle a_1 a_i, a_j \rangle$ 既不交换也不正规, 矛盾.

设 i 是使 $[a_i,a_2]\neq 1$ 的最大的正整数.

(i) 若 $i=1$, 即对所有的 $4\leqslant j\leqslant r$, 都有 $[a_1,a_j]=[a_2,a_j]=[a_3,a_j]=1$, 则 $G\cong K\times A$, 其中 A 是满足 $\exp(A)\leqslant p^{m_3}$ 的交换群. 从而我们得到了定理中的 (2) 型群当 $m_1\geqslant m_2=m_3$ 的情形.

(ii) 若 $i>1$, 则 $m_1>m_i$, 并且对所有的 $i<j\leqslant r$, 都有 $[a_1,a_j]=[a_2,a_j]=[a_3,a_j]=1$. 我们断言 $m_1=m_2$. 若否, 子群 $\langle a_1a_2,a_i\rangle$ 既不交换也不正规, 矛盾. 令 $J=\langle a_2,a_3,a_i\rangle$, 则 J 同构于定理 7.1.3 中的 (7) 型群当 $m_1=m_2>m_3$ 的情况. 对于 $1\leqslant k<i$, 若 $[a_k,a_2]\neq 1$, 用 $a_ka_i^{-1}$ 替换 a_k, 我们可不妨设 $[a_1,a_k]=[a_2,a_k]=[a_3,a_k]=1$. 这种情形下, $G\cong J\times A$, 其中 A 是满足 $\exp(A)=p^{m_2}$ 的交换群. 从而我们得到了定理中的 (7) 型群当 $m_1=m_2>m_3$ 且 $\exp(A)=p^{m_2}$ 的情形.

情形 3: K 与定理 7.1.3 中的 (3) 型群同构. 首先, 我们分两种情形来证明 K 外面一定存在 p^{m_4} 阶元.

(a) p 为奇素数或者 $m_2=m_3>1$.

设 $a_4^{p^{m_4}}=a_2^{\alpha p^{m_2}}a_3^{\beta p^{m_3}}$, 则 $(a_4a_2^{-\alpha p^{m_2-m_4}}a_3^{-\beta p^{m_3-m_4}})^{p^{m_4}}=1$.

(b) $p=2$, $m_2=m_3=m_4=1$.

我们断言 a_4、a_4a_2、a_4a_3 和 $a_4a_2a_3$ 中必有一个 2 阶元. 若否, 我们分三种情形得出矛盾. (1): $a_4^2=a_2^2$. 此时, $(a_4a_2)^2=[a_4,a_2]\neq 1$, 所以子群 $L=\langle a_4,a_2\rangle$ 不交换, 从而 $L\trianglelefteq G$, $a_3^2=[a_1,a_2]\in L$, 所以我们可设 $[a_4,a_2]=a_3^2a_2^{2\alpha}$. 若 $[a_4,a_2]=a_3^2a_2^2$, 则子群 $\langle a_1a_4,a_2\rangle$ 既不交换也不正规, 矛盾, 所以只有 $[a_4,a_2]=a_3^2$. 此时 $(a_4a_2)^2=a_3^2$, $(a_4a_2a_3)^2=[a_4a_2,a_3]=[a_4,a_3]\neq 1$, 所以子群 $M=\langle a_4a_2,a_3\rangle$ 不交换, 从而 $M\trianglelefteq G$, $a_2^2=[a_1,a_3]a_3^2\in M$, 所以我们可设 $[a_4,a_3]=a_2^2a_3^{2\alpha}$. 若 $[a_4,a_3]=a_2^2a_3^2$, 则子群 $\langle a_1a_4a_2,a_3\rangle$ 既不交换也不正规, 矛盾, 所以只有 $[a_4,a_3]=a_2^2a_3^2$. 此时 $(a_4a_3)^2=1$, 矛盾. (2): $a_4^2=a_3^2$. 此时, $(a_4a_3)^2=[a_4,a_3]\neq 1$, 所以子群 $L=\langle a_4,a_3\rangle$ 不交换, 从而 $L\trianglelefteq G$, $a_2^2=[a_1,a_3]a_3^2\in L$, 所以我们可设 $[a_4,a_3]=a_2^2a_3^{2\alpha}$. 若 $[a_4,a_3]=a_2^2$, 则子群 $\langle a_1a_4,a_3\rangle$ 既不交换也不正规, 矛盾, 所以只有 $[a_4,a_3]=a_2^2a_3^2$. 此时 $(a_4a_3)^2=a_2^2a_3^2$, $(a_4a_2)^2=a_2^2a_3^2[a_4,a_2]=[a_4a_3,a_2a_3]\neq 1$, 所以子群 $M=\langle a_4a_3,a_2a_3\rangle$ 不交换, 从而 $M\trianglelefteq G$, $a_2^2=[a_1,a_2a_3]\in M$, 所以我们可设 $[a_4,a_2a_3]=a_3^2$ 或 a_2^2. 若 $[a_4,a_2a_3]=a_3^2$, 则子群 $\langle a_1a_4a_3,a_2a_3\rangle$ 既不交换也不正规, 矛盾, 所以只有 $[a_4,a_2a_3]=a_2^2$. 此

时 $(a_4a_2a_3)^2=1$, 矛盾. (3): $a_4^2=a_2^2a_3^2$. 此时, $(a_4a_2a_3)^2=[a_4,a_2a_3]\neq 1$, 所以子群 $L=\langle a_4,a_2a_3\rangle$ 不交换, 从而 $L\trianglelefteq G$, $a_2^2=[a_1,a_2a_3]\in L$, 所以我们可设 $[a_4,a_2a_3]=a_3^2$ 或 a_2^2. 若 $[a_4,a_2a_3]=a_3^2$, 则子群 $\langle a_1a_4,a_2a_3\rangle$ 既不交换也不正规, 矛盾, 所以只有 $[a_4,a_2a_3]=a_2^2$. 此时 $(a_4a_2a_3)^2=a_2^2$, $(a_4a_3)^2=a_2^2[a_4,a_3]=[a_4,a_2]\neq 1$, 所以子群 $M=\langle a_4a_2a_3,a_2\rangle$ 不交换, 从而 $M\trianglelefteq G$, $a_3^2=[a_1,a_2]\in M$, 所以我们可设 $[a_4,a_2]=a_3^2a_2^{2\alpha}$. 若 $[a_4,a_2]=a_2^2a_3^2$, 则子群 $\langle a_1a_4a_2a_3,a_2\rangle$ 既不交换也不正规, 矛盾, 所以只有 $[a_4,a_2]=a_3^2$. 此时 $(a_4a_2)^2=1$, 矛盾.

所以断言成立, 我们可不妨设 $a_4^{p^{m_4}}=1$.

考虑子群 $L=\langle a_1,a_4\rangle$. 若 $[a_1,a_4]\neq 1$, 则 L 既不交换也不正规. 所以一定有 $[a_1,a_4]=1$.

我们断言 $[a_3,a_4]\in\langle a_2^{kp^{m_2}}a_3^{-p^{m_3}}\rangle$. 若否, 设 $[a_3,a_4]=(a_2^{kp^{m_2}}a_3^{-p^{m_3}})^\alpha a_3^{\gamma p^{m_3}}$, 其中 $(\gamma,p)=1$. 计算可知子群 $M=\langle a_3,a_4a_1^\alpha\rangle$ 既不交换也不正规, 矛盾.

我们断言 $[a_2,a_4]\in\langle a_3^{p^{m_3}}\rangle$. 若否, 设 $[a_2,a_4]=a_2^{\gamma p^{m_2}}a_3^{\beta p^{m_3}}$, 其中 $(\gamma,p)=1$. 计算可知子群 $N=\langle a_2,a_4a_1^\beta\rangle$, 既不交换也不正规, 矛盾. 所以一定有 $[a_2,a_4]=a_3^{\beta p^{m_3}}$.

令 $\delta=k^{-1}((k+1)\alpha-\beta)$, 则 $k(\alpha-\delta)=\beta-\alpha$. 计算可得

$$
\begin{aligned}
[a_2a_3,a_4a_1^\delta] &= [a_2,a_4][a_2,a_1]^\delta[a_3,a_4][a_3,a_1]^\delta \\
&= a_3^{\beta p^{m_3}}a_3^{-\delta p^{m_3}}(a_2^{kp^{m_2}}a_3^{-p^{m_3}})^\alpha(a_2^{kp^{m_2}}a_3^{-p^{m_3}})^{-\delta} \\
&= a_2^{k(\alpha-\delta)p^{m_2}}a_3^{(\beta-\alpha)p^{m_3}} \\
&= (a_2a_3)^{(\beta-\alpha)p^{m_2}}
\end{aligned}
$$

若 $(a_2a_3)^{(\beta-\alpha)p^{m_2}}\neq 1$, 则子群 $\langle a_2a_3,a_4a_1^\delta\rangle$ 既不交换也不正规, 所以一定有

$$(a_2a_3)^{(\beta-\alpha)p^{m_2}}=1.$$

即 $\beta=\alpha$. 若 $(\beta,p)=1$, 用 $a_4^{-\beta^{-1}}$ 替换 a_4, 我们可不妨设 $[a_4,a_2]=a_3^{p^{m_3}}$, $[a_4,a_3]=a_2^{kp^{m_2}}a_3^{-p^{m_3}}$. 若 $m_1=m_4$, 再用 $a_4a_1^{-1}$ 替换 a_4, 我们可不妨 $[a_1,a_4]=[a_2,a_4]=[a_3,a_4]=1$.

同理, 我们可不妨设 $a_i^{p^{m_i}}=1$, 其中 $i=5,6,\dots,r$. 并且, 同理可不妨设 $[a_1,a_i]=[a_2,a_i]=[a_3,a_i]=1$, 或者当 $m_1>m_i$ 时设 $[a_i,a_1]=1$, $[a_i,a_2]=a_3^{p^{m_3}}$, $[a_i,a_3]=a_2^{kp^{m_2}}a_3^{-p^{m_3}}$.

若 $r \geqslant 5$, 我们还可以证明 $[a_i, a_j] = 1$, 其中 $4 \leqslant i < j \leqslant r$.

设 i 是使 $[a_i, a_2] \neq 1$ 的最大的正整数.

(i) 若 $i = 1$, 即对所有的 $4 \leqslant j \leqslant r$, 都有 $[a_1, a_j] = [a_2, a_j] = [a_3, a_j] = 1$, 则 $G \cong K \times A$, 其中 A 是满足 $\exp(A) \leqslant p^{m_3}$ 的交换群. 从而我们得到定理中的 (3) 型群.

(ii) 若 $i > 1$, 则 $m_1 > m_i$, 并且对所有的 $i < j \leqslant r$, 都有 $[a_1, a_j] = [a_2, a_j] = [a_3, a_j] = 1$. 我们断言 $m_1 = m_2$, 若否, 子群 $\langle a_1a_2, a_i \rangle$ 既不交换也不正规, 矛盾. 令 $J = \langle a_2, a_3, a_i \rangle$, 则 J 同构于定理 7.1.3 中的 (8) 型群. 对于 $1 \leq k < i$, 若 $[a_k, a_2] \neq 1$, 用 $a_k a_i^{-1}$ 替换 a_k, 我们可不妨设 $[a_1, a_k] = [a_2, a_k] = [a_3, a_k] = 1$. 这种情形下, $G \cong J \times A$, 其中 A 是满足 $\exp(A) = p^{m_2}$ 的交换群. 从而我们得到定理中的 (8) 型群当 $\exp(A) = p^{m_2}$ 得情形.

情形 4: K 与定理 7.1.3 中的 (4) 型群同构. 首先, 我们分两种情形来证明 K 外面一定存在 p^{m_4} 阶元.

(a) p 为奇素数或者 $m_2 > 1$.

设 $a_4^{p^{m_4}} = a_1^{\alpha p^{m_1}} a_2^{\beta p^{m_2}}$, 则 $(a_4 a_1^{-\alpha p^{m_1 - m_4}} a_2^{-\beta p^{m_2 - m_4}})^{p^{m_4}} = 1$.

(b) $p = 2$, $m_2 = m_3 = m_4 = 1$.

设 $a_4^2 = a_1^{\alpha 2^{m_1}} a_2^{2\beta}$, 则 $(a_4 a_1^{\alpha 2^{m_1 - 1}})^2 = a_2^{2\beta}$. 所以, 我们可不妨设 $a_4^2 = a_2^2$.

我们断言 a_4a_2, a_4a_3 和 $a_4a_2a_3$ 中必有一个元素 x 使得 $x^2 \in \langle a_1^{2^{m_1}} \rangle$. 从而 x 或 $xa_1^{2^{m_1 - 1}}$ 是二阶元. 若否, 由 $(a_4a_2)^2 = [a_4, a_2] \notin \langle a_1^{2^{m_1}} \rangle$ 可得, 子群 $L = \langle a_4, a_2 \rangle$ 不交换. 从而由定理 6.1.3 得 $a_1^{2^{m_1}} \in L$. 所以我们有 $[a_1, a_2] = a_1^{2^{m_1}} a_2^2$. 此时, 子群 $\langle a_4a_2, a_2a_1^{2^{m_1 - 1}} \rangle$ 既不交换也不正规, 矛盾.

所以断言成立. 我们可不妨设 $a_4^{p^{m_4}} = 1$. 易知此时必有 $[a_3, a_4] = 1$.

我们断言 $[a_1, a_4] \in \langle a_2^{p^{m_2}} \rangle$. 若否, 设 $[a_1, a_4] = a_1^{\gamma p^{m_1}} a_2^{\alpha p^{m_2}}$, 其中 $(\gamma, p) = 1$. 计算可知子群 $M = \langle a_1, a_4 a_3^{-\alpha} \rangle$ 既不交换也不正规, 矛盾. 所以我们可设 $[a_1, a_4] = a_2^{\alpha p^{m_2}}$.

我们断言 $[a_2, a_4] \in \langle a_1^{p^{m_1}} \rangle$. 若否, 设 $[a_2, a_4] = a_2^{\gamma p^{m_2}} a_1^{\beta p^{m_1}}$, 其中 $(\gamma, p) = 1$. 计算可知子群 $N = \langle a_1^{\beta p^{m_1 - m_2}} a_2^{\gamma}, a_4 a_3^{-\alpha} \rangle$ 既不交换也不正规, 矛盾. 所以我们可设 $[a_2, a_4] = a_1^{\beta p^{m_1}}$.

我们再断言 $[a_2, a_4] = 1$. 若否, 则 $(\beta, p) = 1$. 若再有 $m_1 > m_2$, 则子群 $O = \langle a_1a_2, a_4 a_3^{-\alpha} \rangle$ 既不交换也不正规, 矛盾; 若 $m_2 = m_1 > 1$, 则子群

$P = \langle a_1a_2, a_4a_3^{\beta-\alpha}\rangle$ 既不交换也不正规, 矛盾.

若 $m_3 = m_4$, 用 $a_4a_3^{-\alpha}$ 替换 a_4, 我们可不妨设 $[a_1, a_4] = 1$. 若 $m_3 > m_4$ 且 $[a_1, a_4] \neq 1$, 用 a_4 的适当方幂去替换 a_4, 我们可不妨设 $[a_1, a_4] = a_2^{p^{m_2}}$.

同理, 我们可不妨设 $a_i^{p^{m_i}} = 1$, 其中 $i = 5, 6, \ldots, r$. 并且, 同理可不妨设 $[a_2, a_i] = [a_3, a_i] = 1$, $[a_1, a_4] = 1$ 或者当 $m_3 > m_i$ 时设 $[a_1, a_4] = a_2^{p^{m_2}}$.

若 $r \geqslant 5$, 设 $4 \leqslant i < j \leqslant r$. 因为子群 $\langle a_i, a_j\rangle$ 不包含 G', 所以由定理 6.1.3 可知 $[a_i, a_j] = 1$.

设 i 是使 $[a_1, a_i] = a_2^{p^{m_2}}$ 的最大的正整数.

(i) 若 $i = 3$, 即对所有的 $4 \leqslant j \leqslant r$, 都有 $[a_1, a_j] = [a_2, a_j] = [a_3, a_j] = 1$, 则 $G \cong K \times A$, 其中 A 是满足 $\exp(A) \leqslant p^{m_3}$ 的交换群. 从而我们得到定理中的 (4) 型群当 $\exp(A) \leqslant p^{m_3}$ 时的情形.

(ii) 若 $i > 3$, 则 $m_3 > m_i$, 并且对所有的 $i < j \leqslant r$, 都有 $[a_1, a_j] = [a_2, a_j] = [a_3, a_j] = 1$. 令 $J = \langle a_1, a_2, a_i\rangle$, 则 J 仍同构于定理 7.1.3 中的 (4) 型群. 对于 $3 \leqslant k < i$, 若 $[a_1, a_k] \neq 1$, 用 $a_ka_i^{-1}$ 替换 a_k, 我们可不妨设 $[a_1, a_k] = [a_2, a_k] = [a_3, a_k] = 1$. 这种情形下, $G \cong J \times A$, 其中 A 是满足 $p^{m_i} < \exp(A) \leqslant p^{m_2}$ 的交换群. 从而我们得到定理中的 (4) 型群 $\exp(A) > p^{m_3}$ 时的情形.

情形 5: K 与定理 7.1.3 中的 (5) 型群同构. 首先, 我们分两种情形来证明 K 外面一定存在 p^{m_4} 阶元.

(a) p 为奇素数或者 $m_3 > 1$.

设 $a_4^{p^{m_4}} = a_1^{\alpha p^{m_1}} a_3^{\beta p^{m_3}}$, 则 $(a_4a_1^{-\alpha p^{m_1-m_4}} a_3^{-\beta p^{m_3-m_4}})^{p^{m_4}} = 1$.

(b) $p = 2$, $m_3 = m_4 = 1$. 先假设 K 外不存在 2 阶元.

设 $a_4^2 = a_1^{\alpha 2^{m_1}} a_3^{2\beta}$, 则 $(a_4a_1^{\alpha 2^{m_1-1}})^2 = a_3^{2\beta}$. 所以, 我们可不妨设 $a_4^2 = a_3^2$. 此时 $(a_4a_1^{2^{m_1-1}})^2 = a_1^{2^{m_1}} a_3^2$. 因为 a_4a_3 不是 2 阶元, 所以 $[a_4, a_3] = (a_4a_3)^2 \neq 1$. 从而子群 $L = \langle a_4, a_3\rangle$ 正规. 因而 $a_1^{2^{m_1}} = [a_1, a_3] \in L$. 若 $(a_4a_3)^2 = [a_4, a_3] = a_1^{2^{m_1}}$, 则 $(a_4a_3a_1^{2^{m_1-1}})$ 为二阶元, 矛盾. 若 $[a_4, a_3] = a_1^{2^{m_1}} a_3^2$, 则子群 $\langle a_4a_1^{2^{m_1-1}}, a_3a_1^{2^{m_1-1}}\rangle \cong Q_8$ 既不交换也不正规, 矛盾.

所以断言成立, 我们可不妨设 $a_4^{p^{m_4}} = 1$. 易知此时必有 $[a_2, a_4] = 1$. 同理, 也有 $[a_2a_3, a_4] = 1$, 从而 $[a_3, a_4] = 1$.

设 $[a_1, a_4] = a_1^{\alpha p^{m_1}} a_3^{\beta p^{m_3}}$. 若 $(\alpha, p) = 1$, 则子群 $M = \langle a_1, a_4a_2^{beta}\rangle$ 既不

交换也不正规, 矛盾. 所以我们可设 $[a_1, a_4] = a_3^{\beta p^{m_3}}$. 若 $(\beta, p) = 1$, 则子群 $N = \langle a_1, a_2^{beta}a_3a_4\rangle$ 既不交换也不正规, 矛盾. 所以, 一定有 $[a_1, a_4] = 1$.

同理, 我们可不妨设 $a_i^{p^{m_i}} = 1$, 其中 $i = 5, 6, \ldots, r$. 并且, 同理可证明 $[a_1, a_i] = [a_2, a_i] = [a_3, a_i] = 1$.

若 $r \geqslant 5$, 我们还可以证明 $[a_i, a_j] = 1$, 其中 $4 \leqslant i < j \leqslant r$. 这种情形下, $G \cong K \times A$, 其中 A 是满足 $\exp(A) \leqslant p^{m_3}$ 的交换群. 从而我们得到了定理中的 (5) 型群.

情形 6: K 与定理 7.1.3 中的 (6) 型群同构. 首先, 我们分两种情形来证明 K 外面一定存在 p^{m_4} 阶元.

(a) p 为奇素数或者 $m_2 > 1$.

设 $a_4^{p^{m_4}} = a_1^{\alpha p^{m_1}} a_2^{\beta p^{m_2}}$, 则 $(a_4 a_1^{-\alpha p^{m_1 - m_4}} a_2^{-\beta p^{m_2 - m_4}})^{p^{m_4}} = 1$.

(b) $p = 2$, $m_2 = m_3 = m_4 = 1$. 此时 $m_1 = 2$. 先假设 K 外不存在 2 阶元.

设 $a_4^2 = a_1^{4\alpha} a_2^{2\beta}$, 则 $(a_4 a_1^{2\alpha})^2 = a_2^{2\beta}$. 所以, 我们可不妨设 $a_4^2 = a_2^2$. 此时 $(a_4 a_1^2)^2 = a_1^4 a_2^2$. 因为 $a_4 a_2$ 不是 2 阶元, 所以 $[a_4, a_2] = (a_4 a_2)^2 \neq 1$, 因而由定理 6.1.3 可得 $a_1^4 \in \langle a_2, a_4\rangle$. 若 $(a_4 a_2)^2 = [a_4, a_2] = a_1^4$, 则 $(a_4 a_2 a_1^2)$ 为二阶元, 矛盾. 若 $[a_4, a_2] = a_1^4 a_2^2$, 则子群 $\langle a_4 a_1^2, a_2 a_1^2\rangle \cong Q_8$ 既不交换也不正规, 矛盾.

所以断言成立, 我们可不妨设 $a_4^{p^{m_4}} = 1$. 易知此时必有 $[a_3, a_4] = 1$.

我们断言 $[a_1, a_4] \in \langle a_2^{p^{m_2}}\rangle$. 若否, 设 $[a_1, a_4] = a_1^{\gamma p^{m_1}} a_2^{\alpha p^{m_2}}$, 其中 $(\gamma, p) = 1$. 则子群 $M = \langle a_1, a_4 a_3^{-\alpha}\rangle$ 既不交换也不正规, 矛盾. 所以我们可设 $[a_1, a_4] = a_2^{\alpha p^{m_2}}$.

我们断言 $[a_2, a_4] \in \langle a_1^{p^{m_1}}\rangle$. 若否, 设 $[a_2, a_4] = a_2^{\gamma p^{m_2}} a_1^{\beta p^{m_1}}$, 其中 $(\gamma, p) = 1$. 则子群 $N = \langle a_2, a_4 a_3^{-\beta}\rangle$ 既不交换也不正规, 矛盾. 所以我们可设 $[a_2, a_4] = a_1^{\beta p^{m_1}}$.

我们再断言 $\alpha \equiv \beta \pmod p$. 若否, 则子群 $O = \langle a_1 a_2, a_4 a_3^{-\alpha}\rangle$ 既不交换也不正规, 矛盾.

若 $m_3 = m_4$, 用 $a_4 a_3^{-\alpha}$ 替换 a_4, 我们可不妨设 $[a_1, a_4] = [a_2, a_4] = 1$. 若 $m_3 > m_4$ 且 $[a_1, a_4] \neq 1$, 用 a_4 的适当方幂去替换 a_4, 我们可不妨设 $[a_1, a_4] = a_2^{p^{m_2}}$, 此时必有 $[a_2, a_4] = a_1^{p^{m_1}}$.

同理, 我们可不妨设 $a_i^{p^{m_i}} = 1$, 其中 $i = 5, 6, \ldots, r$. 并且, 同理可不妨设 $[a_3, a_i] = 1$, $[a_1, a_i] = [a_2, a_i] = 1$ 或者当 $m_3 > m_i$ 时不妨设 $[a_1, a_i] = a_2^{p^{m_2}}$ 同

时 $[a_2, a_i] = a_1^{p^{m_1}}$.

若 $r \geqslant 5$, 设 $4 \leqslant i < j \leqslant r$. 因为子群 $\langle a_i, a_j \rangle$ 不包含 G', 所以由定理 6.1.3 可知 $[a_i, a_j] = 1$.

设 i 是使 $[a_1, a_i] = a_2^{p^{m_2}}$ 的最大的正整数.

(i) 若 $i = 3$, 即对所有的 $4 \leqslant j \leqslant r$, 都有 $[a_1, a_j] = [a_2, a_j] = [a_3, a_j] = 1$, 则 $G \cong K \times A$, 其中 A 是满足 $\exp(A) \leqslant p^{m_3}$ 的交换群. 从而我们得到定理中的 (6) 型群当 $\exp(A) \leqslant p^{m_3}$ 时的情形.

(ii) 若 $i > 3$, 则 $m_3 > m_i$ 并且对所有的 $i < j \leqslant r$, 都有 $[a_1, a_j] = [a_2, a_j] = [a_3, a_j] = 1$. 令 $J = \langle a_1, a_2, a_i \rangle$, 则 J 仍同构于定理 7.1.3 中的 (6) 型群. 对于 $3 \leqslant k < i$, 若 $[a_1, a_k] \neq 1$, 用 $a_k a_i^{-1}$ 替换 a_k, 我们可不妨设 $[a_1, a_k] = [a_2, a_k] = [a_3, a_k] = 1$. 这种情形下, $G \cong J \times A$, 其中 A 是满足 $p^{m_i} < \exp(A) \leqslant p^{m_2}$ 的交换群. 从而我们得到定理中的 (6) 型群当 $\exp(A) > p^{m_3}$ 时的情形.

情形 7: K 与定理 7.1.3 中的 (7) 型群同构.

设 $a_4^{p^{m_4}} = a_1^{\alpha p^{m_1}} a_2^{\beta p^{m_2}}$, 则

$$(a_4 a_1^{-\alpha p^{m_1 - m_4}} a_2^{-\beta p^{m_2 - m_4}})^{p^{m_4}} = 1.$$

我们用 $a_4 a_1^{-\alpha p^{m_1 - m_4}} a_2^{-\beta p^{m_2 - m_4}}$ 来替换 a_4, 仍然有其它的关系成立. 所以, 我们可不妨设 $a_4^{p^{m_4}} = 1$. 易知此时必有 $[a_3, a_4] = 1$.

我们断言 $[a_1, a_4] \in \langle a_2^{p^{m_2}} \rangle$. 若否, 设 $[a_1, a_4] = a_1^{\gamma p^{m_1}} a_2^{\alpha p^{m_2}}$, 其中 $(\gamma, p) = 1$. 则子群 $M = \langle a_1, a_4 a_3^{-\alpha} \rangle$ 既不交换也不正规, 矛盾. 所以我们可设 $[a_1, a_4] = a_2^{\alpha p^{m_2}}$.

我们断言 $[a_2, a_4] \in \langle a_1^{p^{m_1}} \rangle$. 若否, 设 $[a_2, a_4] = a_2^{\gamma p^{m_2}} a_1^{\beta p^{m_1}}$, 其中 $(\gamma, p) = 1$. 则子群 $N = \langle a_2, a_4 a_3^{-\nu^{-1}\beta} \rangle$ 既不交换也不正规, 矛盾. 所以我们可设 $[a_2, a_4] = a_1^{\beta p^{m_1}}$.

我们再断言 $\alpha\nu \equiv \beta \pmod p$. 若否, 则子群 $O = \langle a_1 a_2, a_4 a_3^{-\alpha} \rangle$ 既不交换也不正规, 矛盾.

若 $m_3 = m_4$, 用 $a_4 a_3^{-\alpha}$ 替换 a_4, 我们可不妨设 $[a_1, a_4] = 1$. 若 $m_3 > m_4$ 且 $[a_1, a_4] \neq 1$, 用 a_4 的适当方幂去替换 a_4, 我们可不妨设 $[a_1, a_4] = a_2^{p^{m_2}}$, 此时必有 $[a_2, a_4] = a_1^{\nu p^{m_1}}$.

同理, 我们可不妨设 $a_i^{p^{m_i}}=1$, 其中 $i=5,6,\ldots,r$. 并且, 同理可不妨设 $[a_3,a_i]=1$, $[a_1,a_i]=[a_2,a_i]=1$ 或者当 $m_3>m_i$ 时不妨设 $[a_1,a_i]=a_2^{p^{m_2}}$ 同时 $[a_2,a_i]=a_1^{\nu p^{m_1}}$.

若 $r\geqslant 5$, 设 $4\leqslant i<j\leqslant r$. 因为子群 $\langle a_i,a_j\rangle$ 不包含 G', 所以由定理 6.1.3 可知 $[a_i,a_j]=1$.

设 i 是使 $[a_1,a_i]=a_2^{p^{m_2}}$ 的最大的正整数.

(i) 若 $i=3$, 即对所有的 $4\leqslant j\leqslant r$, 都有 $[a_1,a_j]=[a_2,a_j]=[a_3,a_j]=1$, 则 $G\cong K\times A$, 其中 A 是满足 $\exp(A)\leqslant p^{m_3}$ 的交换群. 从而我们得到定理中的 (7) 型群当 $\exp(A)\leqslant p^{m_3}$ 时的情形.

(ii) 若 $i>3$, 则 $m_3>m_i$ 并且对所有的 $i<j\leqslant r$, 都有 $[a_1,a_j]=[a_2,a_j]=[a_3,a_j]=1$. 令 $J=\langle a_1,a_2,a_i\rangle$, 则 J 仍同构于定理 7.1.3 中的 (7) 型群. 对于 $3\leqslant k<i$, 若 $[a_1,a_k]\neq 1$, 用 $a_ka_i^{-1}$ 替换 a_k, 我们可不妨设 $[a_1,a_k]=[a_2,a_k]=[a_3,a_k]=1$. 这种情形下, $G\cong J\times A$, 其中 A 是满足 $p^{m_i}<\exp(A)\leqslant p^{m_2}$ 的交换群. 从而我们得到定理中的 (7) 型群当 $\exp(A)>p^{m_3}$ 时的情形. 当 $m_1=m_2>m_3$ 时, A 还满足 $\exp(A)<p^{m_2}$.

情形 8: K 与定理 7.1.3 中的 (8) 型群同构.

设 $a_4^{p^{m_4}}=a_1^{\alpha p^{m_1}}a_2^{\beta p^{m_2}}$, 则

$$(a_4a_1^{-\alpha p^{m_1-m_4}}a_2^{-\beta p^{m_2-m_4}})^{p^{m_4}}=1.$$

我们用 $a_4a_1^{-\alpha p^{m_1-m_4}}a_2^{-\beta p^{m_2-m_4}}$ 来替换 a_4, 仍然有其它的关系成立. 所以, 我们可不妨设 $a_4^{p^{m_4}}=1$. 易知此时必有 $[a_3,a_4]=1$.

我们断言 $[a_1,a_4]\in\langle a_2^{p^{m_2}}\rangle$. 若否, 设 $[a_1,a_4]=a_1^{\gamma p^{m_1}}a_2^{\alpha p^{m_2}}$, 其中 $(\gamma,p)=1$. 则子群 $M=\langle a_1,a_4a_3^{-\alpha}\rangle$ 既不交换也不正规, 矛盾. 所以我们可设 $[a_1,a_4]=a_2^{\alpha p^{m_2}}$.

我们断言 $[a_2,a_4]\in\langle a_1^{kp^{m_1}}a_2^{-p^{m_2}}\rangle$. 若否, 设 $[a_2,a_4]=a_2^{\gamma p^{m_2}}(a_1^{kp^{m_1}}a_2^{-p^{m_2}})^{\beta}$, 其中 $(\gamma,p)=1$. 则子群 $N=\langle a_2,a_4a_3^{-\beta}\rangle$ 既不交换也不正规, 矛盾. 所以我们可设 $[a_2,a_4]=(a_1^{kp^{m_1}}a_2^{-p^{m_2}})^{\beta}$.

我们再断言 $\alpha\equiv\beta\pmod p$. 若否, 则子群 $O=\langle a_1a_2,a_4a_3^{-\alpha}\rangle$ 既不交换也不正规, 矛盾.

若 $m_3=m_4$, 用 $a_4a_3^{-\alpha}$ 替换 a_4, 我们可不妨设 $[a_1,a_4]=1$. 若 $m_3>m_4$ 且 $[a_1,a_4]\neq 1$, 用 a_4 的适当方幂去替换 a_4, 我们可不妨设 $[a_1,a_4]=a_2^{p^{m_2}}$, 此

时必有 $[a_2, a_4] = a_1^{kp^{m_1}} a_2^{-p^{m_2}}$.

同理, 我们可不妨设 $a_i^{p^{m_i}} = 1$, 其中 $i = 5, 6, \ldots, r$. 并且, 同理可不妨设 $[a_3, a_i] = 1$, $[a_1, a_i] = [a_2, a_i] = 1$ 或者当 $m_3 > m_i$ 时不妨设 $[a_1, a_i] = a_2^{p^{m_2}}$ 同时 $[a_2, a_i] = a_1^{kp^{m_1}} a_2^{-p^{m_2}}$.

若 $r \geqslant 5$, 设 $4 \leqslant i < j \leqslant r$. 因为子群 $\langle a_i, a_j \rangle$ 不包含 G', 所以由定理 6.1.3 可知 $[a_i, a_j] = 1$.

设 i 是使 $[a_1, a_i] = a_2^{p^{m_2}}$ 的最大的正整数.

(i) 若 $i = 3$, 即对所有的 $4 \leqslant j \leqslant r$, 都有 $[a_1, a_j] = [a_2, a_j] = [a_3, a_j] = 1$, 则 $G \cong K \times A$, 其中 A 是满足 $\exp(A) \leqslant p^{m_3}$ 的交换群. 从而我们得到定理中的 (8) 型群当 $\exp(A) \leqslant p^{m_3}$ 的情形.

(ii) 若 $i > 3$, 则 $m_3 > m_i$ 并且对所有的 $i < j \leqslant r$, 都有 $[a_1, a_j] = [a_2, a_j] = [a_3, a_j] = 1$. 令 $J = \langle a_1, a_2, a_i \rangle$, 则 J 仍同构于定理 7.1.3 中的 (8) 型群. 对于 $3 \leqslant k < i$, 若 $[a_1, a_k] \neq 1$, 用 $a_k a_i^{-1}$ 替换 a_k, 我们可不妨设 $[a_1, a_k] = [a_2, a_k] = [a_3, a_k] = 1$. 这种情形下, $G \cong J \times A$, 其中 A 是满足 $p^{m_i} < \exp(A) < p^{m_2}$ 的交换群. 从而我们得到定理中的 (8) 型群当 $p^{m_3} < \exp(A) < p^{m_2}$ 的情形. □

定理 7.1.5. *下面的群都是有限亚 Hamilton p 群, $c(G) = 2$, G' 为 p^3 阶初等交换 p 群. 不同类型是互不同构的, 同一类型对于不同的参数 (m_1, m_2, m_3) 或者不同的交换群 A 也是互不同构的. 为了研究方便, 我们把它们分为 4 种类型:*

(1a) $G = K \times A$. 其中 $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3+1}} = 1, [a_1, a_2] = a_3^{p^{m_3}}, [a_1, a_3] = a_2^{\nu p^{m_2}}, [a_2, a_3] = a_1^{p^{m_1}} \rangle$, 其中 p 为奇素数, ν 是一个固定的模 p 的平方非剩余, $m_1 = m_2 = m_3 + 1$; A 是满足 $\exp(A) \leqslant p^{m_3}$ 的交换群;

(1b) $G = K \times A$. 其中 $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3+1}} = 1, [a_1, a_2] = a_3^{p^{m_3}}, [a_1, a_3] = a_1^{p^{m_1}} a_2^{lp^{m_2}}, [a_2, a_3] = a_1^{p^{m_1}} \rangle$, 其中 $m_1 = m_2 = m_3 + 1$. 若 $p = 2$, 则 $l = 1$; 若 $p > 2$, 则 $4l = g^{2r+1} - 1$, $r = 1, 2, \ldots, \frac{1}{2}(p-1)$, g 是模 p 的最小原根; A 是满足 $\exp(A) \leqslant p^{m_3}$ 的交换群;

(2) $G = K \times A$. 其中 $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3+1}} =$

$1, [a_1, a_2] = a_3^{p^{m_3}}, [a_1, a_3] = a_2^{\nu p^{m_2}}, [a_2, a_3] = a_1^{p^{m_1}}\rangle$. 其中 p 为奇素数. ν 是一个固定的模 p 的平方非剩余. $m_1 = m_2 + 1 = m_3 + 1$; A 是满足 $\exp(A) \leqslant p^{m_3}$ 的交换群;

(3) $G = K \times A$. 其中 $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3+1}} = 1, [a_1, a_2] = a_3^{p^{m_3}}, [a_1, a_3] = a_2^{kp^{m_2}} a_3^{-p^{m_3}}, [a_2, a_3] = a_1^{p^{m_1}}\rangle$. 其中 $m_1 = m_2 + 1 = m_3 + 1$. 若 p 为奇素数, 则 $1 + 4k$ 是模 p 的平方非剩余; 若 $p = 2$, 则 $k = 1$; A 是满足 $\exp(A) \leqslant p^{m_3}$ 的交换群;

(4) $G = K \times A$. 其中 $K = \langle a_1, a_2, a_3 \mid a_1^4 = a_2^4 = a_3^4 = 1, [a_1, a_2] = a_3^2, [a_1, a_3] = a_2^2 a_3^2, [a_2, a_3] = a_1^2 a_2^2\rangle$; $\exp(A) \leqslant 2$.

证明　我们首先证明定理中的群的二元生成的非交换子群都正规, 从而由定理 6.1.1 可知 G 为有限亚 Hamilton p 群. 对于这些群, 我们都有 $Z(G) = \Phi(K) \times A$. 从而 G 的所有二元生成的非交换子群只可能为以下几种: 第一种, $N = \langle a_2 x, a_3 y\rangle$, 其中 $x, y \in Z(G)$; 第二种, $N = \langle a_1 a_2^i x, a_3 y\rangle$, 其中 $x, y \in Z(G)$; 第三种, $N = \langle a_1 a_3^j x, a_2 a_3^k y\rangle$, 其中 $x, y \in Z(G)$. 下面我们分情况讨论:

(1a) 型群的讨论:

第一种, $N = \langle a_2 x, a_3 y\rangle$, 其中 $x, y \in Z(G)$. 此时, $N' = \langle a_1^{p^{m_1}}\rangle$. 易知 $a_2^{p^{m_2}} = (a_2 x)^{p^{m_2}} \in N$. 又因为 $y^{p^{m_3}} \in \langle a_1^{p^{m_1}}, a_2^{p^{m_2}}\rangle \leqslant N$, 所以 $a_3^{p^{m_3}} = (a_3 y)^{p^{m_3}} y^{-p^{m_3}} \in N$, 从而 $G' \leqslant N$, $N \trianglelefteq G$.

第二种, $N = \langle a_1 a_2^i x, a_3 y\rangle$, 其中 $x, y \in Z(G)$. 此时, $N' = \langle a_1^{ip^{m_1}} a_2^{\nu p^{m_2}}\rangle$. 易知 $a_1^{p^{m_1}} a_2^{ip^{m_2}} = (a_1 a_2^i x)^{p^{m_2}} \in N$. 因为 ν 是一个模 p 的平方非剩余, 所以 $\langle a_1^{p^{m_1}}, a_2^{p^{m_2}}\rangle = \langle a_1^{p^{m_1}} a_2^{ip^{m_2}}, a_1^{ip^{m_1}} a_2^{\nu p^{m_2}}\rangle \leqslant N$. 又因为 $y^{p^{m_3}} \in \langle a_1^{p^{m_1}}, a_2^{p^{m_2}}\rangle \leqslant N$, 所以

$$a_3^{p^{m_3}} = (a_3 y)^{p^{m_3}} y^{-p^{m_3}} \in N.$$

从而 $G' \leqslant N$, $N \trianglelefteq G$.

第三种, $N = \langle a_1 a_3^j x, a_2 a_3^k y\rangle$, 其中 $x, y \in Z(G)$. 此时,

$$N' = \langle a_1^{-jp^{m_1}} a_2^{k\nu p^{m_2}} a_3^{p^{m_3}}\rangle.$$

又因为 $a_1^{p^{m_1}} = (a_1 a_3^j x)^{p^{m_1}} \in N$ 和 $a_2^{p^{m_2}} = (a_2 a_3^k y)^{p^{m_2}} \in N$, 所以 $G' \leqslant N$, 从而 $N \trianglelefteq G$.

(1b) 型群的讨论:

第一种, $N=\langle a_2x, a_3y\rangle$, 其中 $x, y\in Z(G)$. 此时, $N'=\langle a_1^{p^{m_1}}\rangle$. 易知 $a_2^{p^{m_2}}=(a_2x)^{p^{m_2}}\in N$. 又因为 $y^{p^{m_3}}\in\langle a_1^{p^{m_1}}, a_2^{p^{m_2}}\rangle\leqslant N$, 所以 $a_3^{p^{m_3}}=(a_3y)^{p^{m_3}}y^{-p^{m_3}}\in N$, 从而 $G'\leqslant N$, $N\trianglelefteq G$.

第二种, $N=\langle a_1a_2^lx, a_3y\rangle$, 其中 $x, y\in Z(G)$. 此时, $N'=\langle a_1^{(1+l)p^{m_1}}a_2^{lp^{m_2}}\rangle$. 易知 $a_1^{p^{m_1}}a_2^{lp^{m_2}}=(a_1a_2^lx)^{p^{m_2}}\in N$. 因为 $1+4l$ 是一个模 p 的平方非剩余, 所以关于 i 的同余方程 $i^2+i-l\equiv 0\pmod p$ 无解. 从而 $\langle a_1^{p^{m_1}}, a_2^{p^{m_2}}\rangle=\langle a_1^{p^{m_1}}a_2^{lp^{m_2}}, a_1^{(1+l)p^{m_1}}a_2^{lp^{m_2}}\rangle\leqslant N$. 又因为 $y^{p^{m_3}}\in\langle a_1^{p^{m_1}}, a_2^{p^{m_2}}\rangle\leqslant N$, 所以 $a_3^{p^{m_3}}=(a_3y)^{p^{m_3}}y^{-p^{m_3}}\in N$, 从而 $G'\leqslant N$, $N\trianglelefteq G$.

第三种, $N=\langle a_1a_3^jx, a_2a_3^ky\rangle$, 其中 $x, y\in Z(G)$. 此时,

$$N'=\langle a_1^{(k-j)p^{m_1}}a_2^{klp^{m_2}}a_3^{p^{m_3}}\rangle.$$

又因为 $a_1^{p^{m_1}}=(a_1a_3^jx)^{p^{m_1}}\in N$ 和 $a_2^{p^{m_2}}=(a_2a_3^ky)^{p^{m_2}}\in N$, 所以 $G'\leqslant N$, 从而 $N\trianglelefteq G$.

(2) 型群的讨论:

第一种, $N=\langle a_2x, a_3y\rangle$, 其中 $x, y\in Z(G)$. 此时, $N'=\langle a_1^{p^{m_1}}\rangle$. 因为 $x^{p^{m_2}}\in\langle a_1^{p^{m_1}}\rangle=N'$ 和 $y^{p^{m_3}}\in\langle a_1^{p^{m_1}}\rangle=N'$, 所以有 $a_2^{p^{m_2}}=(a_2x)^{p^{m_2}}x^{-p^{m_2}}\in N$ 和 $a_3^{p^{m_3}}=(a_3y)^{p^{m_3}}y^{-p^{m_3}}\in N$, 从而 $G'\leqslant N$, $N\trianglelefteq G$.

第二种, $N=\langle a_1a_2^lx, a_3y\rangle$, 其中 $x, y\in Z(G)$. 此时, $N'=\langle a_1^{lp^{m_1}}a_2^{\nu p^{m_2}}\rangle$. 易知 $a_1^{p^{m_1}}=(a_1a_2^lx)^{p^{m_1}}\in N$, 从而 $\langle a_1^{p^{m_1}}, a_2^{p^{m_2}}\rangle\leqslant N$. 又因为 $y^{p^{m_3}}\in\langle a_1^{p^{m_1}}\rangle\leqslant N$, 所以 $a_3^{p^{m_3}}=(a_3y)^{p^{m_3}}y^{-p^{m_3}}\in N$. 从而 $G'\leqslant N$, $N\trianglelefteq G$.

第三种, $N=\langle a_1a_3^jx, a_2a_3^ky\rangle$, 其中 $x, y\in Z(G)$. 此时,

$$N'=\langle a_1^{-jp^{m_1}}a_2^{k\nu p^{m_2}}a_3^{p^{m_3}}\rangle.$$

易知 $a_1^{p^{m_1}}=(a_1a_3^jx)^{p^{m_1}}\in N$, 从而 $a_2^{k\nu p^{m_2}}a_3^{p^{m_3}}\in N$. 因为 $y^{p^{m_3}}\in\langle a_1^{p^{m_1}}\rangle\leqslant N$, 所以 $a_2^{p^{m_2}}a_3^{kp^{m_3}}=(a_2a_3^ky)^{p^{m_3}}y^{-p^{m_3}}\in N$. 又因为 ν 是一个模 p 的平方非剩余, 所以 $\langle a_2^{p^{m_2}}, a_3^{p^{m_3}}\rangle=\langle a_2^{p^{m_2}}a_3^{kp^{m_3}}, a_2^{k\nu p^{m_2}}a_3^{p^{m_3}}\rangle\leqslant N$. 所以 $G'\leqslant N$, 从而 $N\trianglelefteq G$.

(3) 型群的讨论:

第一种, $N=\langle a_2x, a_3y\rangle$, 其中 $x, y\in Z(G)$. 此时, $N'=\langle a_1^{p^{m_1}}\rangle$. 因为 $x^{p^{m_2}}\in\langle a_1^{p^{m_1}}\rangle=N'$ 和 $y^{p^{m_3}}\in\langle a_1^{p^{m_1}}\rangle=N'$, 所以有 $a_2^{p^{m_2}}=(a_2x)^{p^{m_2}}x^{-p^{m_2}}\in N$ 和 $a_3^{p^{m_3}}=(a_3y)^{p^{m_3}}y^{-p^{m_3}}\in N$, 从而 $G'\leqslant N$, $N\trianglelefteq G$.

第二种, $N=\langle a_1a_2^ix, a_3y\rangle$, 其中 $x,y\in Z(G)$. 此时,

$$N'=\langle a_1^{ip^{m_1}}a_2^{kp^{m_2}}a_3^{-p^{m_3}}\rangle.$$

易知 $a_1^{p^{m_1}}=(a_1a_2^ix)^{p^{m_1}}\in N$, 从而 $\langle a_1^{p^{m_1}}, a_2^{kp^{m_2}}a_3^{-p^{m_3}}\rangle\leqslant N$. 又因为 $y^{p^{m_3}}\in\langle a_1^{p^{m_1}}\rangle\leqslant N$, 所以 $a_3^{p^{m_3}}=(a_3y)^{p^{m_3}}y^{-p^{m_3}}\in N$. 从而 $G'\leqslant N$, $N\trianglelefteq G$.

第三种, $N=\langle a_1a_3^jx, a_2a_3^ly\rangle$, 其中 $x,y\in Z(G)$. 此时,

$$N'=\langle a_1^{-jp^{m_1}}a_2^{klp^{m_2}}a_3^{(1-l)p^{m_3}}\rangle.$$

因为 $a_1^{p^{m_1}}=(a_1a_3^jx)^{p^{m_1}}\in N$, 所以 $\langle a_1^{p^{m_1}}, a_2^{klp^{m_2}}a_3^{(1-l)p^{m_3}}\rangle$. 因为 $y^{p^{m_3}}\in\langle a_1^{p^{m_1}}\rangle\leqslant N$, 所以 $a_2^{p^{m_2}}a_3^{lp^{m_3}}=(a_2a_3^ly)^{p^{m_3}}y^{-p^{m_3}}\in N$. 又因为 $1+4k$ 是一个模 p 的平方非剩余, 所以关于 l 的同余方程 $kl^2+l-1\equiv 0\pmod p$ 无解, 从而 $\langle a_2^{p^{m_2}}, a_3^{p^{m_3}}\rangle=\langle a_2^{p^{m_2}}a_3^{lp^{m_3}}, a_2^{klp^{m_2}}a_3^{(1-l)p^{m_3}}\rangle\leqslant N$. 所以 $G'\leqslant N$, 从而 $N\trianglelefteq G$.

(4) 型群的讨论略.

下面我们说明这些群都是互不同构的.

首先, 因为这些群都有 $G/G'\cong\langle\bar a_1\rangle\times\langle\bar a_2\rangle\times\langle\bar a_3\rangle\times A$, 所以, 如果有两个群同构, 必有相同的参数 m_1, m_2, m_3 以及同构的交换群 A. 因此, 我们只剩下两种情况需要证明:

一. (2) 型群与 (3) 型群互不同构.

对于 (2) 型群, $G/\mho_{m_1}(G)$ 与定理 7.1.2 中的 (Ib) 型群同构; 对于 (3) 型群, $G/\mho_{m_1}(G)$ 与定理 7.1.2 中的 (Ic) 型群同构. 所以 (2) 型群与 (3) 型群也互不同构.

二. (1a) 型群与 (1b) 型群互不同构, 并且不同参数 l 对应得 (1b) 型群也互不同构.

我们只需要处理 p 为奇素数的情形. 令 $m=m_3$, 将这两种类型群中的 K 用统一的形式写成: $K=\langle a_1,a_2,a_3\mid a_1^{p^{m+2}}=a_2^{p^{m+2}}=a_3^{p^{m+1}}=1, [a_1,a_2]=a_3^{p^m}, [a_2,a_3]=a_1^{p^m}, [a_1,a_3]=a_1^{ip^m}a_2^{jp^m}\rangle$, 其中 i^2+4j 是模 p 的平方非剩余.

设 $G=\langle a_1,a_2,a_3,A\rangle$ 和 $\bar G=\langle\bar a_1,\bar a_2,\bar a_3,\bar A\rangle$ 是满足以上条件的两个群, 参数分别为 (i,j) 和 (i',j'). 若 $\bar G$ 与 G 同构, 我们设 θ 是一个从 $\bar G$ 到 G 的同构映射. 因为 $\Omega_{m+1}(G)$, $Z(G)$ 以及 $\Omega_{m+1}(\bar G)$ 和 $Z(\bar G)$ 是 G 或 $\bar G$ 的特征子群, 我们有 $\Omega_{m+1}(\bar G)^\theta=\Omega_{m+1}(G)$, $Z(\bar G)^\theta=Z(G)$.

从而, 我们可设 $\bar{a}_3^\theta = a_3^t x$, $\bar{a}_2^\theta = a_1^s a_2^r y$, $\bar{a}_1^\theta = a_1^v a_2^u z$, 其中 $x \in Z(G)$, $y, z \in \Omega_{m+1}(G)$, $t, rv - us$ 都与 p 互素.

由 $[\bar{a}_2^\theta, \bar{a_3}^\theta] = [\bar{a}_2, \bar{a_3}]^\theta = (\bar{a_1}^{p^{m+1}})^\theta$ 可得

$$[a_1^s a_2^r y, a_3^t x] = (a_1^v a_2^u z)^{p^{m+1}}.$$

即 $a_2^{tsjp^{m+1}} a_1^{(tsi+tr)p^{m+1}} = a_1^{vp^{m+1}} a_2^{up^{m+1}}$. 比较指数可得

$$u \equiv tsj \pmod p, v \equiv tsi + tr \pmod p. \tag{1}$$

再由 $[\bar{a}_1^\theta, \bar{a_3}^\theta] = [\bar{a}_1, \bar{a_3}]^\theta = (\bar{a_2}^{j'p^{m+1}} \bar{a}_1^{i'p^{m+1}})^\theta$ 可得

$$[a_1^v a_2^u z, a_3^t x] = (a_1^s a_2^r y)^{j'p^{m+1}} (a_1^v a_2^u z)^{i'p^{m+1}}.$$

即 $a_2^{jtvp^{m+1}} a_1^{(itv+tu)p^{m+1}} = a_2^{(rj'+ui')p^m} a_1^{(sj'+vi')p^{m+1}}$. 比较指数可得到以下式子,

$$\begin{cases} rj' + ui' \equiv jtv \pmod p \\ sj' + vi' \equiv itv + tu \pmod p \end{cases} \tag{2}$$

由 (2) 解得,

$$\begin{vmatrix} r & u \\ s & v \end{vmatrix} j' \equiv \begin{vmatrix} jtv & u \\ tu + itv & v \end{vmatrix} \pmod p$$

$$\begin{vmatrix} r & u \\ s & v \end{vmatrix} i' \equiv \begin{vmatrix} r & jtv \\ s & tu + itv \end{vmatrix} \pmod p$$

将 (1) 代入, 有

$$\begin{aligned} (rv - su)j' &\equiv jtv^2 - tu^2 - ituv \pmod p \\ &\equiv jtv(tsi + tr) - tu(tsj) - it(tsj)v \\ &= (rv - su)jt^2 \end{aligned}$$

$$\begin{aligned} (rv - su)i' &\equiv rtu + ritv - sjtv \pmod p \\ &\equiv rtu + ritv - uv \\ &\equiv rtu + ritv - u(tsi + tr) \\ &= (rv - su)it \end{aligned}$$

由于 $(rv - su, p) = 1$, 我们有 $j' \equiv jt^2 \pmod p$ 和 $i' \equiv it \pmod p$.

因为 (1a) 型群的参数 (i,j) 为 $(0,\nu)$, 而 (1b) 型群的参数 (i',j') 为 $(1,l)$, 不满足上述条件. 所以 (1a) 型群和 (1b) 型群不同构. 容易看出, 当 $i=i'=1$ 时, 满足上述条件的参数也一定满足 $j'\equiv j \pmod p$. 所以两个不同参数 l 的 (1b) 型群也互不同构. □

定理 7.1.6. 设 G 是有限亚 *Hamilton* p 群. 若 G' 是 p^3 阶的初等交换群, $c(G)=2$ 且 $d(G)=3$, 则 G 为定理 7.1.5 中的满足 $d(G)=3$ 的群, 即:

(1a) $G=\langle a_1,a_2,a_3 \mid a_1^{p^{m_1+1}}=a_2^{p^{m_2+1}}=a_3^{p^{m_3+1}}=1,[a_1,a_2]=a_3^{p^{m_3}},[a_1,a_3]=a_2^{\nu p^{m_2}},[a_2,a_3]=a_1^{p^{m_1}}\rangle$, 其中 p 为奇素数, ν 是一个固定的模 p 的平方非剩余, $m_1=m_2=m_3+1$;

(1b) $G=\langle a_1,a_2,a_3 \mid a_1^{p^{m_1+1}}=a_2^{p^{m_2+1}}=a_3^{p^{m_3+1}}=1,[a_1,a_2]=a_3^{p^{m_3}},[a_1,a_3]=a_1^{p^{m_1}}a_2^{lp^{m_2}},[a_2,a_3]=a_1^{p^{m_1}}\rangle$, 其中 $m_1=m_2=m_3+1$. 若 $p=2$, 则 $l=1$; 若 $p>2$, 则 $4l=g^{2r+1}-1$, $r=1,2,\ldots,\frac{1}{2}(p-1)$, g 是模 p 的最小原根;

(2) $G=\langle a_1,a_2,a_3 \mid a_1^{p^{m_1+1}}=a_2^{p^{m_2+1}}=a_3^{p^{m_3+1}}=1,[a_1,a_2]=a_3^{p^{m_3}},[a_1,a_3]=a_2^{\nu p^{m_2}},[a_2,a_3]=a_1^{p^{m_1}}\rangle$, 其中 p 为奇素数, ν 是一个固定的模 p 的平方非剩余, $m_1=m_2+1=m_3+1$;

(3) $G=\langle a_1,a_2,a_3 \mid a_1^{p^{m_1+1}}=a_2^{p^{m_2+1}}=a_3^{p^{m_3+1}}=1,[a_1,a_2]=a_3^{p^{m_3}},[a_1,a_3]=a_2^{kp^{m_2}}a_3^{-p^{m_3}},[a_2,a_3]=a_1^{p^{m_1+1}}\rangle$, 其中 $m_1=m_2+1=m_3+1$, 若 p 为奇素数, 则 $1+4k$ 是模 p 的平方非剩余; 若 $p=2$, 则 $k=1$;

(4) $G=\langle a_1,a_2,a_3 \mid a_1^4=a_2^4=a_3^4=1,[a_1,a_2]=a_3^2,[a_1,a_3]=a_2^2a_3^2,[a_2,a_3]=a_1^2a_2^2\rangle$.

证明 设 G/G' 的型不变量为 $(p^{m_1},p^{m_2},p^{m_3})$, 其中 $m_1\geq m_2\geqslant m_3$, $G/G'=\langle a_1G'\rangle\times\langle a_2G'\rangle\times\langle a_3G'\rangle$, 其中 $o(a_iG')=p^{m_i}$, $i=1,2,3$. 则 $G=\langle a_1,a_2,a_3\rangle$. 若 $m_1=1$, 则 G 是 p^6 阶群, 此时由定理 6.1.3 可知, G 的非交换子群只能是 p^5 阶群, 从而 G 是 $\mathcal{A}_2$ 群. 由定理 4.6.1 可知, G 只能是定理中的 (4) 型群. 以下我们设 $m_1>1$.

因为 $|G'|=p^3$, 所以 $G'=\langle[a_1,a_2]\rangle\times\langle[a_1,a_3]\rangle\times\langle[a_2,a_3]\rangle$. 令 $x=[a_2,a_3]$, $\bar{G}=G/\langle x\rangle$, $\bar{a}_i=a_i\langle x\rangle$, 其中 $i=1,2,3$. 则 $\bar{G}$ 满足定理 7.1.3 的条件, 并且满

足 $[\bar{a}_2,\bar{a}_3]=\bar{1}$. 从而由定理 7.1.3 的证明过程可知 $\bar{G}$ 只可能为定理 7.1.3 中的 (1)-(5) 型群. 若 $\bar{G}$ 为定理 7.1.3 中的 (4) 型或 (5) 型群, 则子群 $\langle a_2,a_3\rangle$ 既不交换也不正规. 所以 $\bar{G}$ 只可能为定理 7.1.3 中的 (1)-(3) 型群. 以下我们分三种情形讨论:

情形 1: $\bar{G}$ 与定理 7.1.3 中的 (1) 型群同构.

此时 $m_1\geqslant m_2=m_3+1$, $G=\langle a_1,a_2,a_3\rangle$ 满足以下关系:

$$a_1^{p^{m_1}}=x^i, a_2^{p^{m_2+1}}=a_3^{p^{m_3+1}}=1,$$

$$[a_1,a_2]=a_3^{p^{m_3}}x^j,[a_1,a_3]=a_2^{p^{m_2}}x^k,[a_2,a_3]=x.$$

由定理 6.1.3, $G'=\langle a_2^{p^{m_2}},a_3^{p^{m_3}},x\rangle$ 在每个非交换子群中, 所以 $(i,p)=1$, 即 $G'=\langle a_1^{p^{m_1}},a_2^{p^{m_2}},a_3^{p^{m_3}}\rangle$.

我们断言 $m_1=m_2$. 若否, 则子群 $L=\langle a_2,a_3a_1^p\rangle$ 既不交换也不正规, 矛盾.

计算可得, $(a_3a_1^{i^{-1}jp})^{p^{m_3}}=a_3^{p^{m_3}}x^j$. 用 $a_3a_1^{i^{-1}jp}$ 替换 a_3, 我们可不妨设 $[a_1,a_2]=a_3^{p^{m_3}}$. 此时我们有

$$[a_1,a_2]=a_3^{p^{m_3}},[a_1,a_3]=a_2^{p^{m_2}}a_1^{kp^{m_1}},[a_2,a_3]=a_1^{i^{-1}p^{m_1}}.$$

为了运算方便, 我们再添加一个参数, 不妨设 $G=\langle a_1,a_2,a_3\rangle$ 满足以下关系:

$$[a_1,a_2]=a_3^{p^{m_3}},[a_1,a_3]=a_1^{ip^{m_1}}a_2^{jp^{m_2}},[a_2,a_3]=a_1^{kp^{m_1}}.$$

其中, $(j,p)=1,(k,p)=1$.

设 G 的非交换的两个元素分别为 $x=a_1^\alpha a_2^\beta a_3^\gamma g$ 和 $y=a_2^\sigma a_3^\tau h$, 其中 $\alpha,\beta,\gamma,\sigma,\tau=0,1,\ldots,p-1$, $g,h\in\Phi(G)$. 若 $\alpha=0$, 易验证 $\langle x,y\rangle$ 包含 G', 从而正规. 若 $(\alpha,p)=1$, 可不妨设 $\alpha=1$. 此时, 若 $(\sigma,p)=1$, 也可验证 $\langle x,y\rangle$ 包含 G', 从而正规. 当 $\sigma=0$ 时, 又可不妨设 $\tau=1$ 且 $\gamma=0$, 即 $x=a_1a_2^\beta g, y=a_3h$. 计算可得 $[x,y]=a_1^{(i+k\beta)p^{m_1}}a_2^{jp^{m_2}}$. 设 $h^{p^{m_3}}=a_1^{cp^{m_1}}a_2^{dp^{m_2}}$, 则 $G'\leqslant\langle x,y\rangle$ 当且仅当对所有的 β,

$$\begin{vmatrix} i+k\beta & j & 0 \\ 1 & \beta & 0 \\ c & d & 1 \end{vmatrix}\not\equiv 0 \pmod p.$$

即关于 β 的同余方程 $k\beta^2+i\beta-j\equiv 0 \pmod p$ 无解. 若 $p=2$, 由于 $j=k=1$, 所以必有 $i=1$, 从而 G 定理中的 (1b) 型群当 $p=2$ 的情形.

以下设 p 为奇素数, 则上述同余方程无解等价于 i^2+4kj 为模 p 的平方非剩余.

设 $b_1=a_1^r a_2^s a_3^t, b_2=a_1^u a_2^v a_3^w, b_3=a_3^x$ 其中 $x=rv-su$, 其中 r,s,t,u,v,w 是一些合适的非负整数且 $p\nmid x$, 则仍有 $[b_1,b_2]=b_3^{p^{m_3}}$. 计算可得

$$[b_1,b_3]=[a_1^r a_2^s,a_3]^x=a_1^{x(ri+sk)p^{m_1}}a_2^{xrjp^{m_2}},[b_2,b_3]=a^{x(ui+vk)p^{m_1}}a_2^{xujp^{m_2}}.$$

设 $[b_1,b_3]={b_1}^{i_1p^{m_2}}{b_2}^{j_1p^{m_1}}$ 和 $[b_2,b_3]={b_1}^{k_1p^{m_1}}$. 则有 $i_1^2+4k_1j_1$ 是模 p 的平方非剩余, 且

$$\begin{cases} x(ri+sk)\equiv ri_1+uj_1 \pmod p & (1)\\ xrj\equiv si_1+vj_1 \pmod p & (2)\\ x(ui+vk)\equiv rk_1 \pmod p & (3)\\ xuj\equiv sk_1 \pmod p & (4)\end{cases}$$

即

$$x\begin{pmatrix} r & s\\ u & v\end{pmatrix}\begin{pmatrix} i & j\\ k & 0\end{pmatrix}\equiv\begin{pmatrix} i_1 & j_1\\ k_1 & 0\end{pmatrix}\begin{pmatrix} r & s\\ u & v\end{pmatrix} \pmod p.$$

则 $x^2\begin{vmatrix} i & j\\ k & 0\end{vmatrix}\equiv\begin{vmatrix} i_1 & j_1\\ k_1 & 0\end{vmatrix} \pmod p$. 因此 $k_1j_1\equiv x^2kj \pmod p$. 也有

$$\begin{pmatrix} i_1 & j_1\\ k_1 & 0\end{pmatrix}\equiv x\begin{pmatrix} r & s\\ u & v\end{pmatrix}\begin{pmatrix} i & j\\ k & 0\end{pmatrix}\begin{pmatrix} r & s\\ u & v\end{pmatrix}^{-1} \pmod p,$$

即 $\begin{pmatrix} i_1 & j_1\\ k_1 & 0\end{pmatrix}\equiv x\begin{pmatrix} r & s\\ u & v\end{pmatrix}\begin{pmatrix} i & j\\ k & 0\end{pmatrix}\begin{pmatrix} v & -s\\ -u & r\end{pmatrix}x^{-1} \pmod p$,

即 $\begin{pmatrix} i_1 & j_1\\ k_1 & 0\end{pmatrix}\equiv\begin{pmatrix} rvi+svk-ruj & -rsi-s^2k+r^2j\\ uvi+v^2k-u^2j & -sui-svk+ruj\end{pmatrix} \pmod p$. 则

$$\begin{cases} i_1\equiv rvi+svk-ruj \pmod p & (5)\\ j_1\equiv -rsi-s^2k+r^2j \pmod p & (6)\\ k_1\equiv uvi+v^2k-u^2j \pmod p & (7)\\ 0\equiv -sui-svk+ruj \pmod p & (8)\end{cases}$$

由 (5) 和 (8) 得到

$$i_1 \equiv ix \pmod p \qquad (5')$$

子情形 1: $i=0$. 则 $i_1=0$ 和 $k_1 \equiv v^2k-u^2j \pmod p, j_1 \equiv r^2j-s^2k \pmod p$.

(i): k 是模 p 的平方剩余. 则 j 是一个模 p 的平方非剩余. 在此情形, 存在整数 v_0, r_0 满足 $v_0^2k \equiv 1 \pmod p$ 和 $r_0^2j \equiv \nu \pmod p$, 其中 ν 是一个固定的模 p 的平方非剩余. 令 $r=r_0, v=v_0$ 和 $u=s=0$, 得到 $k_1=1$ 和 $j_1=\nu$. 则 $G=\langle b_1,b_2,b_3\rangle$ 与定理中的 (1a) 型群同构.

(ii): k 是模 p 的平方非剩余. 则 j 是模 p 的平方剩余. 在此情形, 存在整数 v_0, u_0 满足 $v_0^2k \equiv \eta \pmod p$ 和 $u_0^2j \equiv 1 \pmod p$, 其中 η 是一个最小的模 p 的平方非剩余 (也就是说, $\eta-1$ 是一个模 p 的平方剩余).

令 $r=u_0\eta, s=v=v_0$ 和 $u=u_0$, 计算可得 $k_1=\eta-1$ 是模 p 的平方剩余, 从而转化为 (i).

子情形 2: $(i,p)=1$.

(i): k 是模 p 的平方剩余. 设 $v=v_0$ 满足 $kv_0^2=1$. 令 $r=i^{-1}kv_0, v=v_0$ 和 $s=u=0$, 则我们有 $x=i^{-1}, i_1=1, k_1=1, j_1=i^{-2}kj$. 从而 $G=\langle b_1,b_2,b_3\rangle$ 与定理中的 (1b) 型群同构, 其中 $l \equiv i^{-2}kj \pmod p$.

(ii): k 是模 p 的平方非剩余且 $-j$ 是一个模 p 的平方剩余. 令 $-j=e^2$, $r=u=ej^{-1}, s=ei^{-1}, v=0$. 则我们有 $x=i^{-1}, i_1=1, k_1=1, j_1=i^{-2}kj$. 从而 $G=\langle b_1,b_2,b_3\rangle$ 与定理中的 (1b) 型群同构, 其中 $l \equiv i^{-2}kj \pmod p$.

(iii): k 和 $-j$ 都是模 p 的平方非剩余. 设 η 是最小的模 p 的平方非剩余, 也就是说, $\eta-1$ 是模 p 的平方剩余. 在此情形, 存在整数 v_0, r_0 满足 $v_0^2k \equiv \eta \pmod p$ 和 $-r_0^2j \equiv \eta \pmod p$. 因为 i^2+4kj 模 p 的平方非剩余, 所以 $\eta(i^2+4kj)$ 是一个平方. 设 $\eta(i^2-4\eta^2)=e^2, r=r_0^2v_0(i-e), s=-2v_0\eta, u=-2r_0\eta, v=r_0v_0^2(i+e)$. 则 $x=-r_0^3v_0^3\eta^{-1}e^2(\eta-1)$. 计算可得 $k_1=r_0^2v_0^2e^2(\eta-1)$ 是一个模 p 的平方剩余, 从而可转化为 (i).

情形 2: $\bar{G}$ 与定理 7.1.3 中的 (2) 型群同构.

此时 p 为奇素数, ν 是一个固定的模 p 的平方非剩余. $G=\langle a_1,a_2,a_3\rangle$ 满足以下关系:

$$a_1^{p^{m_1}}=x^i, a_2^{p^{m_2+1}}=a_3^{p^{m_3+1}}=1,$$

$$[a_1,a_2]=a_3^{p^{m_3}}x^j,[a_1,a_3]=a_2^{\nu p^{m_2}}x^k,[a_2,a_3]=x.$$

若 $m_1\geqslant m_2=m_3+1$, 与情形 1 类似可证明 G 与定理中的 (1a) 型或 (1b) 型群同构. 以下我们设 $m_1\geqslant m_2=m_3$.

由定理 6.1.3, $G'=\langle a_2^{p^{m_2}},a_3^{p^{m_3}},x\rangle$ 在每个非交换子群中, 所以 $(i,p)=1$, 即 $G'=\langle a_1^{p^{m_1}},a_2^{p^{m_2}},a_3^{p^{m_3}}\rangle$.

我们首先证明 $m_1\neq m_2$. 若否, 则存在一组参数 i,j,k 使得 G 是有限亚 Hamilton p 群. 计算可得 $[a_1a_2^\beta,a_3]=a_2^{\nu p^{m_2}}x^{k+\beta}$. 由定理 6.1.3, $G'\leqslant\langle a_1a_2^\beta,a_3\rangle$, 从而关于 β 的同余方程

$$\begin{vmatrix} i & \beta \\ k+\beta & \nu \end{vmatrix}\not\equiv 0 \pmod p \tag{1}$$

无解. 又因为 $[a_1a_3^\gamma,a_2a_3^\tau]=x^{j-\gamma}a_2^{\tau\nu}a_3^{p^{m_3}}$, 同理可得关于 γ 和 τ 的同余方程

$$\begin{vmatrix} j-\gamma+\tau k & \tau\nu & 1 \\ i & 0 & \gamma \\ 0 & 1 & \tau \end{vmatrix}\not\equiv 0 \pmod p \tag{2}$$

无解.

令 $H=\langle a_1,a_2,a_3,x\mid a_1^p=x^i,a_2^{p^2}=a_3^{p^2}=1,[a_1,a_2]=a_3^px^j,[a_1,a_3]=a_2^{\nu p}x^k,[a_2,a_3]=x\rangle$. 由同余方程 (1) 和 (2) 无解可知 H 也是有限亚 Hamilton p 群. 此时由定理 6.1.3 可知, H 的非交换子群只能是 p^5 阶群, 从而 H 是 $\mathcal{A}_2$ 群, 这与定理 4.6.1 矛盾.

我们断言 $m_1=m_2+1$. 若否, 则子群 $L=\langle a_2,a_3a_1^p\rangle$ 既不交换也不正规, 矛盾.

计算可得

$$(a_3a_1^{i^{-1}jp})^{p^{m_3}}=a_3^{p^{m_3}}x^j,(a_2a_1^{i^{-1}k\nu^{-1}p})^{p^{m_2}}=a_2^{p^{m_3}}x^{k\nu^{-1}}.$$

分别用 $a_2a_1^{i^{-1}k\nu^{-1}p}$ 和 $a_3a_1^{i^{-1}jp}$ 替换 a_2 和 a_3, 我们可不妨设 $[a_1,a_2]=a_3^{p^{m_3}}$, $[a_1,a_3]=a_2^{\nu p^{m_2}}$.

此时, 若 i 是一个模 p 的平方剩余, 令 $i=e^2$, 以 a_2^e 和 a_3^e 分别替换 a_2 和 a_3, 我们可得定理中的 (2) 型群; 若 i 是一个模 p 的平方非剩余, 则存在 e 使得 $i\nu=e^2$. 设 $\alpha^2\nu$ 是一个模 p 的最小的平方非剩余, 则 $\alpha^2\nu-1$ 是一个模 p 的平

方剩余. 再设 $\alpha^2\nu - 1 = \beta^2\nu^2$. 以 $a_2^{e\alpha}a_3^{e\beta}$ 和 $a_2^{e\beta\nu}a_3^{e\alpha}$ 分别替换 a_2 和 a_3, 我们可得定理中的 (2) 型群.

情形 3: $\bar{G}$ 与定理 7.1.3 中的 (3) 型群同构.

此时 $m_1 \geqslant m_2 = m_3$, $G = \langle a_1, a_2, a_3\rangle$ 满足以下关系:

$$a_1^{p^{m_1}} = x^i, a_2^{p^{m_2+1}} = a_3^{p^{m_3+1}} = 1,$$

$$[a_1, a_2] = a_3^{p^{m_3}}x^j, [a_1, a_3] = a_2^{kp^{m_2}}a_3^{-p^{m_3}}x^l, [a_2, a_3] = x.$$

由定理 6.1.3, $G' = \langle a_2^{p^{m_2}}, a_3^{p^{m_3}}, x\rangle$ 在每个非交换子群中, 所以 $(i, p) = 1$. 即 $G' = \langle a_1^{p^{m_1}}, a_2^{p^{m_2}}, a_3^{p^{m_3}}\rangle$.

我们首先证明 $m_1 \neq m_2$. 若否, 则存在一组参数 i, j, l 使得 G 是有限亚 Hamilton 群. 若 p 为奇素数, 仿照情形 2 的证明可以得出矛盾. 当 $p = 2$ 时, i 一定为 1. j, l 为 0 或 1. 若 $j = 0$, 由于 $[a_1a_3, a_2] = a_1^{2^{m_1}}a_3^{2^{m_3}}$, 子群 $\langle a_1a_3, a_2\rangle$ 既不交换也不正规, 矛盾; 若 $j = 1, l = 0$, 由于 $[a_1a_2a_3, a_3] = a_1^{2^{m_1}}a_2^{2^{m_2}}a_3^{2^{m_3}}$, 子群 $\langle a_1a_2a_3, a_3\rangle$ 既不交换也不正规, 矛盾; 若 $j = l = 1$, 由于 $[a_1a_2, a_2a_3] = a_1^{2^{m_1}}a_2^{2^{m_2}}$, 子群 $\langle a_1a_2, a_2a_3\rangle$ 既不交换也不正规, 同样可以得出矛盾.

此时, 若 i 是一个模 p 的平方剩余, 令 $i = e^2$, 以 a_2^e 和 a_3^e 分别替换 a_2 和 a_3, 我们可得定理中的 (3) 型群; 若 i 是一个模 p 的平方非剩余 (此时 p 为奇素数), 则存在 e 使得 $i = e^2(1 + 4k)$. 设 η 是一个模 p 的最小的平方非剩余, 则 $\eta - 1$ 是一个模 p 的平方剩余. 再设 $\eta - 1 = d^2$, $\eta(1 + 4k) = f^2$. 以 $a_2^{e(f+d)}a_3^{2de}$ 和 $a_2^{2dek}a_3^{e(f-d)}$ 分别替换 a_2 和 a_3, 我们可得定理中的 (3) 型群.

定理 7.1.7. *设 G 是有限亚 Hamilton p 群, G' 为 p^3 阶初等交换群且 $c(G) = 2$, 则 G 为定理 7.1.5 中的群, 即:*

(1a) *$G = K \times A$, 其中 $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3+1}} = 1, [a_1, a_2] = a_3^{p^{m_3}}, [a_1, a_3] = a_2^{\nu p^{m_2}}, [a_2, a_3] = a_1^{p^{m_1}}\rangle$, 其中 p 为奇素数, ν 是一个固定的模 p 的平方非剩余, $m_1 = m_2 = m_3 + 1$; A 是满足 $\exp(A) \leqslant p^{m_3}$ 的交换群;*

(1b) *$G = K \times A$, 其中 $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3+1}} = 1, [a_1, a_2] = a_3^{p^{m_3}}, [a_1, a_3] = a_1^{p^{m_1}}a_2^{lp^{m_2}}, [a_2, a_3] = a_1^{p^{m_1}}\rangle$, 其中 $m_1 = m_2 = m_3 + 1$. 若 $p = 2$, 则 $l = 1$; 若 $p > 2$, 则 $4l = g^{2r+1} - 1$,*

$r = 1, 2, \ldots, \frac{1}{2}(p-1)$, g 是模 p 的最小原根; A 是满足 $\exp(A) \leqslant p^{m_3}$ 的交换群;

(2) $G = K \times A$. 其中 $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3+1}} = 1, [a_1, a_2] = a_3^{p^{m_3}}, [a_1, a_3] = a_2^{\nu p^{m_2}}, [a_2, a_3] = a_1^{p^{m_1}} \rangle$, 其中 p 为奇素数, ν 是一个固定的模 p 的平方非剩余, $m_1 = m_2 + 1 = m_3 + 1$; A 是满足 $\exp(A) \leqslant p^{m_3}$ 的交换群;

(3) $G = K \times A$. 其中 $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3+1}} = 1, [a_1, a_2] = a_3^{p^{m_3}}, [a_1, a_3] = a_2^{kp^{m_2}} a_3^{-p^{m_3}}, [a_2, a_3] = a_1^{p^{m_1}} \rangle$, 其中 $m_1 = m_2 + 1 = m_3 + 1$, 若 p 为奇素数, 则 $1 + 4k$ 是模 p 的平方非剩余; 若 $p = 2$, 则 $k = 1$; A 是满足 $\exp(A) \leqslant p^{m_3}$ 的交换群;

(4) $G = K \times A$. 其中 $K = \langle a_1, a_2, a_3 \mid a_1^4 = a_2^4 = a_3^4 = 1, [a_1, a_2] = a_3^2, [a_1, a_3] = a_2^2 a_3^2, [a_2, a_3] = a_1^2 a_2^2 \rangle$; $\exp(A) \leqslant 2$.

证明 设 G/G' 的型不变量为 $(p^{m_1}, p^{m_2}, \ldots, p^{m_r})$, 其中 $m_1 \geqslant m_2 \geq \cdots \geqslant m_r$, $G/G' = \langle a_1 G' \rangle \times \langle a_2 G' \rangle \times \cdots \times \langle a_r G' \rangle$, 其中 $o(a_i G') = p^{m_i}$, $i = 1, 2, \ldots, r$. 则 $G = \langle a_1, a_2, \ldots, a_r \rangle$.

设 i 是使 a_i 不在 $Z(G)$ 中的最小的正整数, 即存在 $j > i$ 使 $[a_i, a_j] \neq 1$. 若 $i \neq 1$, 说明 a_1 在 $Z(G)$ 中, 从而 $[a_1 a_j, a_i] \neq 1$, 此时, 我们可以用 $a_1 a_j$ 来替换 a_1, 仍然有其它的关系成立. 所以, 我们可不妨设 $i = 1$, 即 $a_1 \notin Z(G)$.

再设 j 是使 $[a_1, a_j] \neq 1$ 的最小的正整数. 若 $j \neq 2$, 说明 $[a_1, a_2] = 1$, 从而 $[a_1, a_2 a_j] \neq 1$, 此时, 我们可以用 $a_2 a_j$ 来替换 a_2, 仍然有上面的关系成立. 所以, 我们可不妨设 $j = 1$, 即 $[a_1, a_2] \neq 1$.

再设 k 是使 $[a_k, a_l] \notin \langle [a_1, a_2] \rangle$ 的最小正整数. 若 $k > 2$, 说明对所有的 s 都有 $[a_1, a_s] \in \langle [a_1, a_2] \rangle, [a_2, a_s] \in \langle [a_1, a_2] \rangle$. (1), 如果 $[a_1, a_l] = 1$, 我们有 $[a_1, a_2 a_l] = [a_1, a_2]$, $[a_2 a_l, a_k] = [a_2, a_k][a_l, a_k] \notin \langle [a_1, a_2] \rangle$. 此时, 我们用 $a_2 a_l$ 来替换 a_2, 仍然有其它的关系成立. 所以, 我们可不妨设 $k \leqslant 2$. (2), 如果 $[a_1, a_l] = [a_1, a_2]^\alpha$, 其中 $(\alpha, p) = 1$. 再设 $[a_1, a_k] = [a_1, a_2]^\beta$, 我们有 $[a_1, a_k a_l^{\alpha^{-1}\beta}] = 1$, $[a_1, a_2 a_k a_l^{\alpha^{-1}\beta}] = [a_1, a_2]$, $[a_2 a_k a_l^{\alpha^{-1}\beta}, a_l] = [a_2, a_l][a_k, a_l] \notin \langle [a_1, a_2] \rangle$. 此时, 我们用 $a_2 a_k a_l^{\alpha^{-1}\beta}$ 来替换 a_2, 仍然有其它的关系成立. 所以, 我们可不妨设 $k \leqslant 2$.

再设 l 是使 $[a_k, a_l] \notin \langle [a_1, a_2] \rangle$ 的最小正整数. 若 $l \neq 3$, 说明

$$[a_1, a_3] \in \langle [a_1, a_2] \rangle, [a_2, a_3] \in \langle [a_1, a_2] \rangle.$$

从而 $[a_k, a_3 a_l] = [a_k, a_3][a_k, a_l] \neq 1$, 此时, 我们用 $a_3 a_l$ 来替换 a_3, 仍然有其它的关系成立. 所以, 我们可不妨设 $l = 3$.

令 $K = \langle a_1, a_2, a_3 \rangle$, 则 $|K'| \geqslant p^2$. 若 $|K'| = p^2$, 设 $G' = K' \times \langle z \rangle$. 设 s 是使 $[a_s, a_t] \notin K'$ 的最小正整数. 再设 $H = \langle a_1, a_2, a_3, a_s, a_t \rangle$, $\bar{H} = H/\langle z \rangle$. 则 $\bar{H}$ 为定理 7.1.3 中的一个群. 若 H 是定理 7.1.3 中的 (10) 型群, 不妨设 $H = \langle c_1, c_2, b, d, e \rangle$, 且 $\bar{H} = \langle \bar{c_1}, \bar{c_2}, \bar{b}, \bar{d} \rangle \times \langle \bar{e} \rangle$ 满足定理 7.1.3 中定义关系. 则我们可设 $b^2 = c_1^2 z^i, d^2 = c_2^2 z^j$ 以及

$$[c_1, c_2] = z^k, [c_1, b] = c_2^2 z^l, [c_2, b] = c_1^2 z^m,$$

$$[c_1, d] = c_1^2 z^s, [c_2, d] = c_1^2 c_2^2 z^t, [b, d] = z^r$$

因为 $[c_1, b] \neq 1$, 所以 $G' \leqslant \langle c_1, b \rangle$. 从而 $b^2 \neq c_1^2$, 即 $b^2 = c_1^2 z$. 同理可得 $d^2 = c_2^2 z$, $[c_1, d] = c_1^2 z$. 此时 $(c_1 d)^2 = c_1^2 d^2 [c_1, d] = c_2^2$, $\langle c_1 d, c_2 \rangle$ 不可能包含 G', 由定理 6.1.3 可得 $[c_1 d, c_2] = 1$. 但是 $[c_1 d, c_2] = z^k c_1^2 c_2^2 z^t \neq 1$, 矛盾. 所以 H 只能是定理 7.1.3 中的 (1)–(9) 型群, 不妨设 $H = \langle b_1, b_2, b_3, b_4, b_5 \rangle$, 且 $\bar{H} = \langle \bar{b_1}, \bar{b_2}, \bar{b_3} \rangle \times \langle \bar{b_4}, \bar{b_5} \rangle$ 满足定理 7.1.3 中定义关系. 设 $o(\bar{b_4}) = p^{n_4}$, $o(\bar{b_5}) = p^{n_5}$, 且 $n_4 \geqslant n_5$, 则有 $b_4^{p^{n_4}} = z^u, b_5^{p^{n_5}} = z^v$ 以及 $[b_i, b_4] = z^{u_i}, [b_i, b_5] = z^{v_i}$, 其中 $i = 1, 2, 3$. 由定理 6.1.3 可知, 只有 $[b_i, b_4] = [b_i, b_5] = [b_4, b_5] = 1$. 从而 $|\langle b_1, b_2, b_3 \rangle'| = p^3$. 设 $L = \langle b_1, b_2, b_3 \rangle$, 且 L/G' 的型不变量为 $(p^{n_1}, p^{n_2}, p^{n_3})$, 其中 $n_1 \geqslant n_2 \geqslant n_3$. 若 $n_4 \geqslant n_5 \geqslant n_1$, 则必有 $n_4 = m_1, n_5 = m_2, n_1 = m_3$. 此时, 用 $b_4 b_2, b_5 b_3$ 和 b_1 分别去替换 b_1, b_2 和 b_3, 我们仍有 $|L'| = p^3$, 并且此时 L/G' 有型不变量 $(p^{m_1}, p^{m_2}, p^{m_3})$; 对于 n_i 的其它关系, 我们也可以用类似的替换使得 $|L'| = p^3$, 并且 L/G' 有型不变量 $(p^{m_1}, p^{m_2}, p^{m_3})$.

以上讨论说明, 我们可不妨设 $K = \langle a_1, a_2, a_3 \rangle$ 满足 $|K'| = p^3$. 从而 K 是定理 7.1.6 中的一个群. 由定理 7.1.6 易知 $G' = K' = \langle a_1^{p^{m_1}}, a_2^{p^{m_2}}, a_3^{p^{m_3}} \rangle$. 此时, 对于 $i > 3$, 可设 $a_i^{p^{m_i}} = a_1^{rp^{m_1}} a_2^{sp^{m_2}} a_3^{tp^{m_3}}$. 若 p 为奇数或 $m_3 > 1$, 用

$$a_i a_1^{-rp^{m_1 - m_i}} a_2^{-sp^{m_2 - m_i}} a_3^{-rp^{m_3 - m_i}}$$

替换 a_i, 可不妨设 $a_i^{p^{m_i}}=1$; 若 $p=2$ 且 $m_3=1$, K 可能为定理 7.1.6 中的 (1b) 型群, (3) 型群或者 (4) 型群. (i): 若 K 为定理 7.1.6 中的 (1b) 型群, 可设 $a_i^2=a_1^{4r}a_2^{4s}a_3^{2t}$. 计算可得 $(a_ia_1^{2r}a_2^{2s})^2=a_3^{2t}$. 若 $(a_ia_1^{2r}a_2^{2s})^2\neq 1$, 则必有 $[a_ia_1^{2r}a_2^{2s},a_3]=1$, 从而

$$(a_ia_1^{2r}a_2^{2s}a_3)^2=1.$$

用 $a_ia_1^{2r}a_2^{2s}$ 或 $a_ia_1^{2r}a_2^{2s}a_3$ 替换 a_i, 可不妨设 $a_i^2=1$; (ii): 若 K 为定理 7.1.6 中的 (3) 型群, 可设 $a_i^2=a_1^{4r}a_2^{2s}a_3^{2t}$. 计算可得 $(a_ia_1^{2r})^2=a_2^{2s}a_3^{2t}$. 若 $(a_ia_1^{2r})^2=a_2^2$ 或者 a_3^3, 与 (i) 类似可得 $(a_ia_1^{2r}a_2)^2=1$ 或者 $(a_ia_1^{2r}a_3)^2=1$; 若 $(a_ia_1^{2r})^2=a_2^2a_3^3$, 计算可得 $(a_ia_1^{2r+2})^2=a_1^2a_2^2a_3^2=(a_2a_3)^2$. 则必有 $[a_ia_1^{2r+2},a_2a_3]=1$, 从而 $(a_ia_1^{2r+2}a_2a_3)^2=1$. 所以, 经过适当的替换, 我们可不妨设 $a_i^2=1$; (iii): 若 K 为定理 7.1.6 中的 (4) 型群. 若 $a_i^2\neq 1$, 则存在 K 的生成元 x 使得 $x^2=a_i^2$. 则必有 $[a_i,x]=1$, 从而 $(a_ix)^2=1$. 所以, 经过适当的替换, 我们可不妨设 $a_i^2=1$.

综上所述, 对于 $i>3$, 我们总可以不妨设 $a_i^{p^{m_i}}=1$. 由定理 6.1.3 可知, $a_i\in Z(G)$. 令 $A=\langle a_4,a_5,\ldots,a_r\rangle$, 则 $G=K\times A$. 从而我们得到定理中的群. □

§7.2 导群非初等交换的亚循环的有限亚 Hamilton p 群

下面是本节的主要定理:

定理 7.2.1. *设 G 是亚循环 p- 群, 且 $|G'|\geqslant p^2$. 则 G 是有限亚 Hamilton p 群当且仅当 G 是以下互不同构的群之一:*

(1) $<r,s,t,u>_p$ *满足* $r\geqslant 1$, $u\leqslant r$ *和* $r+1\geqslant s+u\geqslant 2$. *并且若* $p=2$, *则* $r\geqslant 2$;

(2) *16 阶二面体群, 半二面体群和广义四元数群;*

(3) $<r,s,v,t,t',u>_2$ *其中* $r=3,s=v=t'=u=0,t\geqslant 0$;

(4) $<r,s,v,t,t',u>_2$ *其中* $r=2,s+v+t'+u=1,t\geqslant 0$.

其中 (2), (3), (4) 型群可以写成如下的形式, 其中 $m\geqslant 1$:

(2') $\langle a,b \mid a^{2^3}=b^{2^m}=1,a^b=a^{-1}\rangle$;

(3') $\langle a,b \mid a^{2^3}=1,b^{2^m}=a^4,a^b=a^{-1}\rangle$;

(4') $\langle a,b \mid a^{2^3} = b^{2^m} = 1, a^b = a^3\rangle$.

证明　首先我们证明以上四种类型的群都是有限亚 Hamilton p 群. 对于类型 (1), 我们考虑它的二元生成的子群 H, 设 $H = \langle b^{i_1}a^{j_1}, b^{i_2}a^{j_2}\rangle$, 并且不妨设 $b^{i_2} \in \langle b^{i_1}\rangle$. 设 $b^{i_2} = (b^{i_1})^k$, 则 $(b^{i_1}a^{j_1})^{-k}b^{i_2}a^{j_2} \in \langle a\rangle$, 所以, 我们可不妨设 $H = \langle b^{i_1}a^{j_1}, a^l\rangle$. 进一步, 我们可设 $H = \langle b^{p^i}a^j, a^{p^k}\rangle$, 其中, i, j, k 为非负整数. 若 $k \leqslant r$, 则 $G' \leqslant H$, 因而 $H \trianglelefteq G$; 若 $k \geqslant r+1$, 则 $r+k \geqslant r+s+u$, 所以 $[a^{p^k}, b] = a^{-p^k}(a^{p^k})^b = a^{p^{r+k}} = 1$, 因而 $[a^{p^k}, b^{p^i}a^j] = [a^{p^k}, b^{p^i}] = 1$, 即 H 交换. 由于 H 的任意性以及定理 6.1.1 可得 G 为有限亚 Hamilton p 群. 对于其它的类型, 由定理 4.6.1 可知, G 都是 $\mathcal{A}_2$ 群, 当然也是有限亚 Hamilton p 群.

我们再证明 G 一定是以上四种类型之一.

情形 1: 若 p 为奇素数或者 $p = 2$ 且 G 是通常的亚循环群, 由定理 3.2.1 可知, $G = \langle a, b \mid a^{p^{r+s+u}} = 1, b^{p^{r+s+t}} = a^{p^{r+s}}, a^b = a^{1+p^r}\rangle$, 其中 $r \geqslant 1$, $u \leqslant r$, 且若 $p = 2$, 则 $r \geqslant 2$. 因为 $|G'| \geqslant p^2$, 所以 $s+u \geqslant 2$. 下面我们用反证法来证明 $r+1 \geqslant s+u$, 从而 G 是定理中的 (1) 型群.

若 $r+1 < s+u$, 则一定有 $2r+1 < r+s+u$, $s \neq 0$. 计算可得 $[a^{p^{r+1}}, b] = a^{-p^{r+1}}(a^{p^{r+1}})^b = a^{p^{2r+1}} \neq 1$. 所以 G 的子群 $H = \langle a^{p^{r+1}}, b\rangle$ 不交换, 因而一定有 H 正规. 由定理 6.1.3 得 $G' \leqslant H$. 但 $a^{p^r} = [a, b] \notin H$, 矛盾.

情形 2: 若 $p = 2$ 且 G 不是通常的亚循环群, 我们来证明 $|G'| = 2^2$. 注意到不论 G 是哪一种类型都有 $G' = \langle a^2\rangle$, 并且 $\langle [a^{2^k}, b]\rangle = \langle a^{2^{k+1}}\rangle$. 设 $o(a) = 2^n$, 考虑子群 $H = \langle a^{2^{n-2}}, b\rangle$, 因为 H 不交换, 所以必有 H 正规, 从而由定理 6.1.3 可知 $a^2 \in H$. 因而 $n \leqslant 3$, $|G'| \leq 2^2$, G 是定理中的 (2) 型群, (3) 型群或 (4) 型群.

最后, 我们来证明 (2),(3),(4) 型群一定可以写成 $(2')$, $(3')$, $(4')$ 的形式. 易知, (2) 型群中的三个 16 阶的极大类 2 群对应于 $(2') - (4')$ 中 $m = 1$ 的群. (3) 型群对应于 $(2')$ 中 $m \geqslant 3$ 的群. 以下只考虑 (4) 型群. 当 $v = 1$ 时, 由条件可知 $s = t = t' = u = 0$. 此时, 我们得到群 $\langle a, b \mid a^{2^3} = b^{2^2} = 1, a^b = a^{-1}\rangle$, 对应于 $(2')$ 中 $m = 2$ 的群. 当 $v = u = 0$ 时, 我们得到群 $\langle a, b \mid a^{2^3} = 1, b^{2^{2+s+t}} = 1, a^b = a^3\rangle$, 对应于 $(4')$ 中 $m \geqslant 2$ 的群. 当 $v = 0$ 且 $u = 1$ 时, 由条件可知 $s = t' = 0$. 此时, 我们得到群 $\langle a, b \mid a^{2^3} = 1, b^{2^{2+t}} = a^4, a^b = a^3\rangle$. 令 $a_1 = ab^{2^{t+1}}$, 则有 $\langle a, b\rangle = \langle a_1, b \mid a_1^{2^3} = 1, b^{2^{t+2}} = a_1^4, a_1^b = a_1^{-1}\rangle$. 这与 $(3')$ 中

$m \geqslant 2$ 的群相对应. □

§7.3 导群非初等交换的非亚循环的有限亚 Hamilton p 群

下面是本节的主要定理:

定理 7.3.1. 设 G 是有限 p 群, G 不是亚循环群且 G' 不是初等交换群则 G 是亚 Hamilton 群当且仅当 G 是以下互不同构的群之一:

类型 (I): G' 循环的非亚循环的亚 Hamilton p 群, 此时一定有 $d(G) \geqslant 3$. G 有以下几种互不同构的类型:

(1) $G = K \times A$. 其中 $K = \langle a, b \mid a^{p^{r+s+u}} = 1, b^{p^{r+s}} = 1, a^b = a^{1+p^r}\rangle$, $u \leqslant r$, $r+1 > s+u \geqslant 2$, A 是满足 $\exp(A) \leqslant p^{(r+1)-(s+u)}$ 的非平凡的交换群;

(2) $G = K \times A$. 其中 $K = \langle a, b \mid a^{p^{r+t+u}} = 1, b^{p^r} = 1, a^b = a^{1+p^{r+t}}\rangle$, $t \geqslant 1$, $r \geqslant u \geqslant 2$. A 是满足 $\exp(A) \leqslant p^{t+(r+1)-u}$ 的非平凡的交换群;

(3) $G = K \times A$. 其中 $K = \langle a, b \mid a^{p^{r+s}} = 1, b^{p^{r+s+t}} = 1, a^b = a^{1+p^r}\rangle$, $t \geqslant 1$, $r+1 > s \geqslant 2$, A 是满足 $\exp(A) \leqslant p^{(r+1)-s}$ 的非平凡交换群;

(4) $G = K \times A$. 其中 $K = \langle a, b \mid a^{p^{r+s+u}} = 1, b^{p^{r+s+t}} = a^{p^{r+s}}, a^b = a^{1+p^r}\rangle$, $stu \neq 0$, $r+1 > s+u \geqslant 2$, A 是满足 $\exp(A) \leqslant p^{(r+1)-(s+u)}$ 的非平凡交换群;

(5) $G = (K \rtimes B) \times A$. 其中 $K = \langle a, b \mid a^{p^{r+t+u}} = 1, b^{p^r} = 1, a^b = a^{1+p^{r+t}}\rangle$, $B = \langle b_1\rangle \times \langle b_2\rangle \times \cdots \times \langle b_f\rangle$ 满足 $o(b_i) = p^{r_i}$, $[a, b_i] = a^{p^{r+t_i}}$, $[b, b_i] = 1$, $\max\{t, u-2\} < t_1 < t_2 < \cdots < t_f < t+u$, $r+t > r_1+t_1 > r_2+t_2 > \cdots > r_f+t_f \geqslant t+u \geqslant t+2$. A 是满足 $\exp(A) \leqslant p^{t+(r+1)-u}$ 的交换群.

类型 (II): G' 的型不变量为 (p^α, p)(其中 $\alpha \geq 2$) 的亚 Hamilton p 群. G 有以下几种互不同构的类型:

(1) $G = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1+m_2}} = a_2^{p^{m_2+1}} = a_3^p = 1, [a_1, a_2] = a_1^{p^{m_1}}, [a_1, a_3] = a_2^{p^{m_2}}, [a_2, a_3] = 1\rangle$, 其中 $m_1 > m_2 \geqslant 1$, p 为奇素数;

(2) $G = K \times A$. 其中 $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1+k}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3}} = 1, [a_1, a_2] = a_1^{p^{m_1}}, [a_1, a_3] = a_2^{p^{m_2}}, [a_2, a_3] = 1\rangle$, $m_1 \geqslant m_2 \geqslant m_3$, $1 \leqslant k \leq \min\{m_1 - m_3, m_2 - m_3 + 1, m_2 - 1\}$. A 是满足 $\exp(A) \leqslant p^{m_2-k}$ 的交换群.

本节的思路是: 由定理 7.3.2, 定理 7.3.7 和定理 7.3.8 组成定理 7.3.1 的充分性的证明; 由定理 7.3.6 和定理 7.3.9 组成定理 7.3.1 的必要性的证明.

定理 7.3.2. 下面是一些互不同构的有限亚 *Hamilton* p 群, 满足 $|G'| \geqslant p^2$ 且 G' 循环.

(1) $G = K \times A$. 其中 $K = \langle a, b \mid a^{p^{r+s+u}} = 1, b^{p^{r+s}} = 1, a^b = a^{1+p^r}\rangle$, $u \leqslant r$, $r + 1 > s + u \geqslant 2$, A 是满足 $\exp(A) \leqslant p^{(r+1)-(s+u)}$ 的交换群;

(2) $G = K \times A$. 其中 $K = \langle a, b \mid a^{p^{r+t+u}} = 1, b^{p^r} = 1, a^b = a^{1+p^{r+t}}\rangle$, $t \geqslant 1$, $r \geqslant u \geqslant 2$. A 是满足 $\exp(A) \leqslant p^{t+(r+1)-u}$ 的交换群;

(3) $G = K \times A$. 其中 $K = \langle a, b \mid a^{p^{r+s}} = 1, b^{p^{r+s+t}} = 1, a^b = a^{1+p^r}\rangle$, $t \geqslant 1$, $r + 1 > s \geqslant 2$, A 是满足 $\exp(A) \leqslant p^{(r+1)-s}$ 的交换群;

(4) $G = K \times A$. 其中 $K = \langle a, b \mid a^{p^{r+s+u}} = 1, b^{p^{r+s+t}} = a^{p^{r+s}}, a^b = a^{1+p^r}\rangle$, $stu \neq 0$, $r + 1 > s + u \geqslant 2$, A 是满足 $\exp(A) \leqslant p^{(r+1)-(s+u)}$ 的交换群;

(5) $G = (K \rtimes B) \times A$. 其中 $K = \langle a, b \mid a^{p^{r+t+u}} = 1, b^{p^r} = 1, a^b = a^{1+p^{r+t}}\rangle$, $B = \langle b_1\rangle \times \langle b_2\rangle \times \cdots \times \langle b_f\rangle$ 满足 $o(b_i) = p^{r_i}$, $[a, b_i] = a^{p^{r+t_i}}$, $[b, b_i] = 1$, $\max\{t, u-2\} < t_1 < t_2 < \cdots < t_f < t + u$, $r + t > r_1 + t_1 > r_2 + t_2 > \cdots > r_f + t_f \geqslant t + u \geqslant t + 2$. A 是满足 $\exp(A) \leqslant p^{t+(r+1)-u}$ 的交换群;

证明　我首先证明它们都是有限亚 Hamilton p 群, 且 K 是满足 $K' = G'$ 的 G 的最小阶的子群.

对于类型 (1), 我们考虑它的二元生成的子群 H, 设 $H = \langle b^{i_1}a^{j_1}x, b^{i_2}a^{j_2}y\rangle$, 其中 $x, y \in A$. 不妨设 $b^{i_2} \in \langle b^{i_1}\rangle$. 设 $b^{i_2} = (b^{i_1})^k$, 则 $(b^{i_1}a^{j_1}x)^{-k}b^{i_2}a^{j_2}y \in \langle a\rangle \times A$. 所以, 我们可不妨设 $H = \langle b^{i_1}a^{j_1}x, a^l y\rangle$, 其中其中 $x, y \in A$. 进一

步, 我们可设 $H=\langle b^{p^i}a^jx, a^{p^k}y\rangle$, 其中, i,j,k 为非负整数, $x,y\in A$. 计算可得 $(a^{p^k}y)^{p^{(r+1)-(s+u)}}=a^{p^{(r+1)-(s+u)+k}}$. 若 $k\leqslant s+u-1$, 则 $G'\leqslant H$, 因而 $H\trianglelefteq G$; 若 $k\geqslant s+u$, 则 $r+k\geqslant r+s+u$, 所以 $[a^{p^k},b]=a^{-p^k}(a^{p^k})^b=a^{p^{r+k}}=1$, 因而 $[a^{p^k}y,b^{p^i}a^jx]=[a^{p^k},b^{p^i}]=1$, 即 H 交换. 由于 H 的任意性以及定理 6.1.1 可得 G 为有限亚 Hamilton p 群.

容易看出, 若 $H'=G'$, 则 $i=k=0$. 此时, 可不妨设 $H=\langle bx,ay\rangle$, 其中 $x,y\in A$. 不难看出 $H\cong K$, 因此 K 是满足 $K'=G'$ 的 G 的最小阶的子群.

对于类型 (2), 我们考虑它的二元生成的子群 H, 设 $H=\langle b^{i_1}a^{j_1}x,b^{i_2}a^{j_2}y\rangle$, 其中 $x,y\in A$. 不妨设 $b^{i_2}\in\langle b^{i_1}\rangle$. 设 $b^{i_2}=(b^{i_1})^k$, 则 $(b^{i_1}a^{j_1}x)^{-k}b^{i_2}a^{j_2}y\in\langle a\rangle\times A$. 所以, 我们可不妨设 $H=\langle b^{i_1}a^{j_1}x,a^ly\rangle$, 其中 $x,y\in A$. 进一步, 我们可设 $H=\langle b^{p^i}a^jx,a^{p^k}y\rangle$, 其中, i,j,k 为非负整数, $x,y\in A$. 计算可得 $(a^{p^k}y)^{p^{t+(r+1)-u}}=a^{p^{t+(r+1)-u+k}}$. 若 $k\leqslant u-1$, 则 $G'\leqslant H$, 因而 $H\trianglelefteq G$; 若 $k\geqslant u$, 则 $r+t+k\geqslant r+t+u$, 所以 $[a^{p^k},b]=a^{-p^k}(a^{p^k})^b=a^{p^{r+t+k}}=1$, 因而 $[a^{p^k}y,b^{p^i}a^jx]=[a^{p^k},b^{p^i}]=1$, 即 H 交换. 由于 H 的任意性以及定理 6.1.1 可得 G 为有限亚 Hamilton p 群.

容易看出, 若 $H'=G'$, 则 $i=k=0$, 此时, 可不妨设 $H=\langle bx,ay\rangle$, 其中 $x,y\in A$. 不难看出 K 是满足 $K'=G'$ 的 G 的最小阶的子群.

对于类型 (3), 我们考虑它的二元生成的子群 H, 设 $H=\langle b^{i_1}a^{j_1}x,b^{i_2}a^{j_2}y\rangle$, 其中 $x,y\in A$. 不妨设 $b^{i_2}\in\langle b^{i_1}\rangle$. 设 $b^{i_2}=(b^{i_1})^k$, 则 $(b^{i_1}a^{j_1}x)^{-k}b^{i_2}a^{j_2}y\in\langle a\rangle\times A$. 所以, 我们可不妨设 $H=\langle b^{i_1}a^{j_1}x,a^ly\rangle$, 其中 $x,y\in A$. 进一步, 我们可设 $H=\langle b^{p^i}a^jx,a^{p^k}y\rangle$, 其中, i,j,k 为非负整数, $x,y\in A$. 计算可得 $(a^{p^k}y)^{p^{(r+1)-s}}=a^{p^{(r+1)-s+k}}$. 若 $k\leqslant s-1$, 则 $G'\leqslant H$, 因而 $H\trianglelefteq G$; 若 $k\geqslant s$, 则 $r+k\geqslant r+s$, 所以 $[a^{p^k},b]=a^{-p^k}(a^{p^k})^b=a^{p^{r+k}}=1$, 因而 $[a^{p^k}y,b^{p^i}a^jx]=[a^{p^k},b^{p^i}]=1$, 即 H 交换. 由于 H 的任意性以及定理 6.1.1 可得 G 为有限亚 Hamilton p 群.

容易看出, 若 $H'=G'$, 则 $i=k=0$, 此时, 可不妨设 $H=\langle bx,ay\rangle$, 其中 $x,y\in A$. 不难看出 $H\cong K$, 因此 K 是满足 $K'=G'$ 的 G 的最小阶的子群.

对于类型 (4), 我们考虑它的二元生成的子群 H, 设 $H=\langle b^{i_1}a^{j_1}x,b^{i_2}a^{j_2}y\rangle$, 其中 $x,y\in A$. 不妨设 $b^{i_2}\in\langle b^{i_1}\rangle$. 设 $b^{i_2}=(b^{i_1})^k$, 则 $(b^{i_1}a^{j_1}x)^{-k}b^{i_2}a^{j_2}y\in\langle a\rangle\times A$. 所以, 我们可不妨设 $H=\langle b^{i_1}a^{j_1}x,a^ly\rangle$, 其中 $x,y\in A$. 进一步,

我们可设 $H = \langle b^{p^i} a^j x, a^{p^k} y\rangle$, 其中, i, j, k 为非负整数, $x, y \in A$. 计算可得 $(a^{p^k} y)^{p^{(r+1)-(s+u)}} = a^{p^{(r+1)-(s+u)+k}}$. 若 $k \leqslant s+u-1$, 则 $G' \leqslant H$, 因而 $H \trianglelefteq G$; 若 $k \geqslant s+u$, 则 $r+k \geqslant r+s+u$, 所以 $[a^{p^k}, b] = a^{-p^k}(a^{p^k})^b = a^{p^{r+k}} = 1$, 因而 $[a^{p^k} y, b^{p^i} a^j x] = [a^{p^k}, b^{p^i}] = 1$, 即 H 交换. 由于 H 的任意性以及定理 6.1.1 可得 G 为有限亚 Hamilton p 群.

容易看出, 若 $H' = G'$, 则 $i = k = 0$, 此时, 可不妨设 $H = \langle bx, ay\rangle$, 其中 $x, y \in A$. 不难看出 $H \cong K$, 因此 K 是满足 $K' = G'$ 的 G 的最小阶的子群.

对于类型 (5), 我们考虑它的二元生成的子群 H, 设 $H = \langle \rho_1, \rho_1\rangle$, 其中 $\rho_1 = b^{i_1} b_1^{u_1} \dots b_f^{u_f} a^{j_1} x$, $\rho_2 = b^{i_2} b_1^{v_1} \dots b_f^{v_f} a^{j_2} y$, 其中 $x, y \in A$. 不妨设 $b^{i_2} \in \langle b^{i_1}\rangle$. 设 $b^{i_2} = (b^{i_1})^k$, 则 $\rho_1^{-k}\rho_2 \in (\langle a\rangle \rtimes B) \times A$. 所以, 我们可不妨设 $\rho_1 = b^{p^i} b_1^{u_1} \dots b_f^{u_f} a^{jp^\alpha} x, \rho_2 = b_1^{v_1} \dots b_f^{v_f} a^{kp^\beta} y$, 其中, j, k 都与 p 互素, $x, y \in A$.

由 $t_1 \geqslant u-1$ 和 $r+t > t_1 + r_1$ 可得 $r_1 < t + (r+1) - u$. 计算可得 $\rho_1^{p^{(r+1)+t_1-u}} = a^{jp^{(r+1)+t_1-u+\alpha}}$, $\rho_2^{p^{t+(r+1)-u}} = a^{kp^{t+(r+1)-u+\beta}}$. 若 $\alpha \leqslant u+t-t_1-1$ 或者 $\beta \leqslant u-1$, 我们都有 $G' \leqslant H$, 因而 $H \trianglelefteq G$; 若 $\alpha \geqslant u+t-t_1$ 且 $\beta \geqslant u$, 则 $r+t+\beta \geqslant r+s+u$ 且 $r+t_1+\alpha \geqslant r+t+u$, 所以我们有 $[a^{p^\alpha}, b_w] = a^{-p^\alpha}(a^{p^\alpha})^{b_w} = a^{p^{r+t_w+\alpha}} = 1$, $[a^{p^\beta}, b] = a^{-p^\beta}(a^{p^\beta})^b = a^{p^{r+t+\beta}} = 1$, 以及 $[a^{p^\beta}, b_w] = a^{-p^\beta}(a^{p^\beta})^{b_w} = a^{p^{r+t_w+\beta}} = 1$. 因而 $[\rho_1, \rho_2] = 1$, H 交换. 由于 H 的任意性以及定理 6.1.1 可得 G 为有限亚 Hamilton p 群.

容易看出, 若 $H' = G'$, 则 $i = k = 0$, 此时,

$$H = \langle bb_1^{u_1} \dots b_f^{u_f} a^{jp^\alpha} x, b_1^{v_1} \dots b_f^{v_f} ay\rangle,$$

其中 $x, y \in A$. 不难看出 K 是满足 $K' = G'$ 的 G 的最小阶的子群.

下面我们来解决同构问题. 首先, 由于只有 (5) 型群中 K 不是 G 的直积因子, 所以 (5) 型群与其它群不同构.

为了说明 (1),(2),(3),(4) 型群互不同构, 我们先把原来略去的参数补上. 即, 在 (1) 型群中令 $t = 0$, (2) 型群中令 $s = 0$, (3) 型群中令 $u = 0$. 容易知道以下事实:

(i) $|K| = p^{2r+2s+t+u}$;

(ii) $\exp(G) = p^{r+s+t+u}$;

(iii) $\exp(G/G') = p^{r+s+t}$;

(iv) $|G'| = p^{s+u}$.

由以上事实可以知道, r, s, t, u 都是 G 的不变量. 从而不同类型的群互不同构, 并且同一类型的群对于不同的参数 r, s, t, u 也互不同构. 又由于 $G/G' \cong K/K' \times A$, 所以类型 (1), (2), (3), (4) 中相同参数 r, s, t, u 的群对于不同构的交换群 A 也互不同构.

与上面类似可得到 r, t, u 也是 (5) 型群的不变量. 考虑商群 $\tilde{G} = G/\mho_{\delta-t}(G')$. 当 $t < \delta \leqslant t_1$ 时, $\tilde{G}$ 中存在与 $\tilde{G}$ 的导群相同的亚循环的直积因子 $K/\mho_{\delta-t}(G')$; 而 $\delta > t_1$ 时, $\tilde{G}$ 中不存在与 $\tilde{G}$ 的导群相同的亚循环的直积因子; 所以 t_1 也是 G 的不变量. 进一步, 当 $\delta = t_1 + 1$ 时, $\tilde{T} = (K \rtimes \langle b_1 \rangle)/\mho_{\delta-t}(G')$ 是阶最小的与 $\tilde{G}$ 的导群相同的直积因子. 因为 $|\tilde{T}| = p^{2r+t+u+r_1}$, 所以 r_1 也是 G 的不变量. 依次类推, 当 $t_i < \delta \leqslant t_{i+1}$ 时, $\tilde{G}$ 中存在与 $\tilde{G}$ 的导群相同的 $i+2$ 元生成的直积因子 $\tilde{T}_i = (K \rtimes (\langle b_1 \rangle \times \langle b_2 \rangle \ldots \langle b_i \rangle))/\mho_{\delta-t}(G')$; 而 $\delta > t_{i+1}$ 时, $\tilde{G}$ 中不存在与 $\tilde{G}$ 的导群相同的 $i+2$ 元生成的直积因子. 进一步, 当 $\delta = t_{i+1} + 1$ 时, $\tilde{T}_{i+1}$ 是阶最小的与 $\tilde{G}$ 的导群相同的直积因子. 因为 $|\tilde{T}_{i+1}| = p^{2r+t+u+r_1+r_2+\cdots+r_{i+1}}$. 所以由归纳法可知 t_i 和 r_{i+1} 也是 G 的不变量. 这就说明了不同的 $K \rtimes B$ 对应得群不同构. 最后, 由于 $G/G' \cong K/G' \times B \times A$, 不同构的 A 对应的 (5) 型群也互不同构. □

接下来我们需要下面的定理.

定理 7.3.3. *设 G 是二元生成的有限亚 Hamilton p 群, 且 $\exp(G') > p$, 则 G 亚循环.*

Proof. 设 $G = \langle a, b \rangle$ 是极小阶的反例. 由定理 3.1.1, $\overline{G} := G/\Phi(G')G_3$ 非亚循环. 因为 $|\overline{G}'| = p$, $\overline{G}$ 是内交换群. 由定理 2.1.6, $\overline{G} \cong \mathcal{M}_p(n, m, 1)$. 因为 $\langle \bar{a}^p, \bar{b} \rangle$, $\langle \bar{b}^p, \bar{a} \rangle$, $\langle \bar{a}\bar{b}^p, \bar{a} \rangle$, $\langle \bar{a}\bar{b}^p, \bar{b} \rangle$ 均为 $\overline{G}$ 的不正规的子群, 所以它们在 G 中的完全反像也是 G 的不正规的子群, 从而是交换群. 所以我们有:

$$[a^p, b] = [b^p, a] = [(ab)^p, a] = [(ab)^p, b] = 1 \qquad (*)$$

下面我们分两种情况得出矛盾:

(i) $p = 2$. 此时 $(ab)^2 = a^2 b^2 [a, b]$. 由 $(*)$ 式可知, $[a, b] \in Z(G)$, 从而 $G' = \langle [a, b] \rangle$. 再由 $(*)$ 式, $[a, b]^2 = [a^2, b] = 1$. 这与 $\exp(G') > 2$ 矛盾.

(ii) p 为奇素数. 由 $(*)$ 式可得, $[a,b,a]^p=[a^p,b,a]=1$, $[a,b,b]^p=[a^p,b,b]=1$. 即 $\exp(G_3)\leqslant p$. 再由 $(*)$ 式, $[a,b]^p=[a^p,b]=1$. 这与 $\exp(G')>p$ 矛盾. □

我们还需要下面两个初等数论的引理, 证明从略.

引理 7.3.4. 设 p 是奇素数, n 是正整数. 假定 $U=U(p^n)$ 是由 $\mathbb{Z}/p^n\mathbb{Z}$ 的可逆元组成的乘法群, 即

$$U=\{x\in\mathbb{Z}/p^n\mathbb{Z}\mid(x,p)=1\}.$$

设 $S(U)\in\mathrm{Syl}_p(U)$, 则

$$S(U)=\{x\in U\mid x\equiv 1\ (\mathrm{mod}\ p)\},$$

并且 $S(U)$ 是 p^{n-1} 阶循环群. $S(U)$ 的唯一的 p^i 阶子群 $S_i(U), 0\leqslant i<n$, 是

$$S_i(U)=\{x\in U\mid x\equiv 1\ (\mathrm{mod}\ p^{n-i})\}.$$

引理 7.3.5. 设 n 是正整数, $n\geqslant 2$. 假定 $U=U(2^n)$ 是由环 $\mathbb{Z}/2^n\mathbb{Z}$ 的可逆元组成的乘法群, 则

$$\begin{aligned} U &= \langle -1\rangle\times\langle 1+2^2\rangle(\cong C_2\times C_{2^{n-2}})\\ &= \{\varepsilon+i2^m\mid \varepsilon=1\text{或}-1, 2\leqslant m\leqslant n, 1\leqslant i\leqslant 2^{n-m}\text{且}i\text{是奇数}\}\end{aligned}$$

又, 对 $m<n$, $\varepsilon+i2^m$ 的阶是 2^{n-m}. 且 $\langle\varepsilon+i2^m\rangle=\langle\varepsilon+j2^m\rangle$ 对任意的奇数 j 成立.

定理 7.3.6. 设 G 是非亚循环的有限亚 *Hamilton* p 群. 若 $|G'|\geqslant p^2$ 且 G' 循环, 则 G 为以下群之一:

(1) $G=K\times A$. 其中 $K=\langle a,b\mid a^{p^{r+s+u}}=1, b^{p^{r+s}}=1, a^b=a^{1+p^r}\rangle$, $u\leqslant r$, $r+1>s+u\geqslant 2$, A 是满足 $\exp(A)\leqslant p^{(r+1)-(s+u)}$ 的非平凡的交换群;

(2) $G=K\times A$. 其中 $K=\langle a,b\mid a^{p^{r+t+u}}=1, b^{p^r}=1, a^b=a^{1+p^{r+t}}\rangle$, $t\geqslant 1$, $r\geqslant u\geqslant 2$. A 是满足 $\exp(A)\leqslant p^{t+(r+1)-u}$ 的非平凡的交换群;

(3) $G = K \times A$. 其中 $K = \langle a, b \mid a^{p^{r+s}} = 1, b^{p^{r+s+t}} = 1, a^b = a^{1+p^r}\rangle$, $t \geqslant 1$, $r+1 > s \geqslant 2$, A 是满足 $\exp(A) \leqslant p^{(r+1)-s}$ 的非平凡交换群;

(4) $G = K \times A$. 其中 $K = \langle a, b \mid a^{p^{r+s+u}} = 1, b^{p^{r+s+t}} = a^{p^{r+s}}, a^b = a^{1+p^r}\rangle$, $stu \neq 0$, $r+1 > s+u \geqslant 2$, A 是满足 $\exp(A) \leqslant p^{(r+1)-(s+u)}$ 的非平凡交换群;

(5) $G = (K \rtimes B) \times A$. 其中 $K = \langle a, b \mid a^{p^{r+t+u}} = 1, b^{p^r} = 1, a^b = a^{1+p^{r+t}}\rangle$, $B = \langle b_1\rangle \times \langle b_2\rangle \times \cdots \times \langle b_f\rangle$ 满足 $o(b_i) = p^{r_i}$, $[a, b_i] = a^{p^{r+t_i}}$, $[b, b_i] = 1$, $\max\{t, u-2\} < t_1 < t_2 < \cdots < t_f < t+u$, $r+t > r_1+t_1 > r_2+t_2 > \cdots > r_f+t_f \geqslant t+u \geqslant t+2$. A 是满足 $\exp(A) \leqslant p^{t+(r+1)-u}$ 的交换群.

证明 由定理 7.3.3 可知, $d(G) > 2$. 设 $G' = \langle c\rangle$, G/G' 的型不变量为

$$(p^{m_1}, p^{m_2}, \ldots, p^{m_w}),$$

其中 $m_1 \geqslant m_2 \geq \cdots \geqslant m_w$, $G/G' = \langle a_1G'\rangle \times \langle a_2G'\rangle \times \cdots \times \langle a_wG'\rangle$, 其中 $o(a_iG') = p^{m_i}$, $i = 1, 2, \ldots, w$. 则 $G = \langle a_1, a_2, \ldots, a_w\rangle$.

设 i 是使 a_i 不在 $C_G(G/\mho_1(G'))$ 中的最小的正整数, 即存在 $j > i$ 使 $G' = \langle [a_i, a_j]\rangle$. 若 $i \neq 1$, 说明 a_1 在 $C_G(G/\mho_1(G'))$ 中, 从而 $[a_1a_j, a_i] \notin \mho_1(G')$, $G' = \langle a_1a_j, a_i\rangle$. 此时, 用 a_1a_j 来替换 a_1, 我们可不妨设 $i = 1$, 即 $a_1 \notin C_G(G/\mho_1(G'))$.

再设 j 是使 $G' = \langle [a_1, a_j]\rangle$ 的最小的正整数. 若 $j \neq 2$, 说明 $[a_1, a_2] \in \mho_1(G')$. 此时, 用 a_2a_j 来替换 a_2, 我们可不妨设 $j = 2$, 即 $G' = \langle [a_1, a_2]\rangle$.

设 $K = \langle a_1, a_2\rangle$, 则由定理 7.3.3 可知, K 为亚循环群. 从而 K 为定理 7.2.1 中的群. 下面我们分五步来证明定理.

第一步: K 一定是定理 7.2.1 中的 (1) 型群.

若否, 可设 $K = \langle a, b\rangle$ 满足定理 7.2.1 中的 $(2')$, $(3')$ 或 $(4')$ 的关系. 则 $a^{2^3} = 1$, $b^{2^m} \in K_3 = \langle a^4\rangle$, $[a, b] \in \langle a^2\rangle \backslash \langle a^4\rangle$, 并且 $G' = K' = \langle a^2\rangle$, $m_3 = m_4 = \cdots = m_w = 1$. 我们分三种情形来推出矛盾:

情形 1: $a_3^2 \in K_3$ 且 $[a_3, b] \in K_3$.

此时, 若 $[a_3, b] = a^4$, 则子群 $\langle a_3, b\rangle$ 既不交换也不正规, 矛盾; 若 $[a_3, b] = 1$, 则 $[a_3a^2, b] = a^4$, 从而子群 $\langle a_3a^2, b\rangle$ 既不交换也不正规, 矛盾.

情形 2: $a_3^2 \in K_3$ 且 $[a_3, b] \equiv a^2 \pmod{K_3}$.

若 $[a_3, a] \in K_3$. 则 $[a_3, a^2] = [a_3, a]^2 = 1$, 即 $[a_3, G'] = 1$. 计算可得, $1 = [a_3^2, b] = [a_3, b]^2[a_3, b, a_3] = [a_3, b]^2$, 从而 $[a_3, b] \in K_3$, 矛盾. 所以一定有 $[a_3, a] \equiv a^2 \pmod{K_3}$. 此时, $(a_3a)^2 \in K_3$ 且 $[a_3a, b] \in K_3$. 用 a_3a 替换 a_3 可转化为情形 1 得出矛盾.

情形 3: $a_3^2 \equiv a^2 \pmod{K_3}$.

若 $[a_3, a] \in K_3$, 则 $(a_3a)^2 \in K_3$. 此时, 用 a_3a 替换 a_3 可转化为情形 1 或情形 2 得出矛盾. 以下我们不妨设 $[a_3, a] \equiv a^2 \pmod{K_3}$.

因为 $a_3^2 \equiv a^2 \pmod{K_3}$, 所以 $[a_3^2, b] = [a^2, b] = a^4$. 从而必有 $[a_3, b] \equiv a^2 \pmod{K_3}$. 注意到此时 $(a_3a)^2 \equiv a^2 \pmod{K_3}$, 同理有

$$[a_3a, b] \equiv a^2 \pmod{K_3}.$$

这使得 $[a, b] \in K_3$, 矛盾.

第二步: 通过替换, 我们可不妨设 $a_i^{p^{m_i}} = 1$, 其中 $3 \leqslant i \leqslant w$. 从而 $[a_i, a_j] = 1$ 对于 $3 \leqslant i, j \leqslant w$ 成立.

由第一步, $K \cong < r, s, t, u >_p$ 且满足 $r \geqslant 1$, $u \leqslant r$ 和 $r + 1 \geqslant s + u$. 若 $p = 2$, 则还有 $r \geqslant 2$. 设 $K = \langle a, b \mid a^{p^{r+s+u}} = 1, b^{p^{r+s+t}} = a^{p^{r+s}}, a^b = a^{1+p^r} \rangle$.

令 $L = \langle a, a_i \rangle$, 并且设 x_i 是使 $L = \langle a, x_i \rangle$ 成立且 $\langle x_i \rangle \cap \langle a \rangle$ 最小的元素, 我们断言 $x_i^{p^{m_i}} = 1$. 若否, 设 $\langle x_i \rangle \cap \langle a \rangle = \langle a^{p^\alpha} \rangle$, $\langle [x_i, a] \rangle = \langle a^{p^\beta} \rangle$, 其中 $\alpha \geqslant r$, $\beta \geqslant r$. 则存在与 p 互素的整数 y 和 z 使得 $x_i^{p^{m_i}} = a^{yp^\alpha}$, $[x_i, a] = a^{zp^\beta}$. 用命题 1.1.4 计算可得

$$\begin{aligned}(x_i a^{-yp^{\alpha-m_i}})^{p^{m_i}} &= x_i^{p^{m_i}} [x_i, a^{yp^{\alpha-m_i}}]^{\binom{p^{m_i}}{2}} [x_i, a^{yp^{\alpha-m_i}}, x_i]^{\binom{p^{m_i}}{3}} a^{-yp^\alpha} \\ &= a^{yzp^{\alpha+\beta-m_i}\binom{p^{m_i}}{2}} [a^{yzp^{\alpha+\beta-m_i}\binom{p^{m_i}}{3}}, x_i]\end{aligned}$$

注意到当 $p = 2$ 时, $\beta \geqslant r \geqslant 2$, 我们总有 $(x_i a^{-yp^{\alpha-m_i}})^{p^{m_i}} \in \langle a^{p^{\alpha+1}} \rangle$, 这与 x_i 的取法矛盾.

用上面的 x_i 去替换 a_i, 我们可不妨设 $a_i^{p^{m_i}} = 1$, 其中 $3 \leqslant i \leqslant w$. 对于 $3 \leqslant i, j \leqslant w$, 因为 $\langle a_i, a_j \rangle$ 不包含 G', 所以由定理 6.1.3 可知 $[a_i, a_j] = 1$.

第三步: 将 K 按是否可裂分别写成如下的四种群:

(I) $K = \langle a, b \mid a^{p^{r+s+u}} = 1, b^{p^{r+s}} = 1, a^b = a^{1+p^r} \rangle$, 其中 $r+1 \geqslant s+u \geqslant 2$, 且若 $p = 2$ 则 $r \geqslant 2$;

(II) $K = \langle a, b \mid a^{p^{r+t+u}} = 1, b^{p^r} = 1, a^b = a^{1+p^{r+t}} \rangle$, 其中 $t \geqslant 1$, $r \geqslant u \geqslant 2$;

(III) $K = \langle a, b \mid a^{p^{r+s}} = 1, b^{p^{r+s+t}} = 1, a^b = a^{1+p^r} \rangle$, 其中 $t \geqslant 1$, $r + 1 \geqslant s \geqslant 2$, 且若 $p = 2$ 则 $r \geqslant 2$;

(IV) $K = \langle a, b \mid a^{p^{r+s+u}} = 1, b^{p^{r+s+t}} = a^{p^{r+s}}, a^b = a^{1+p^r} \rangle$. 其中, $stu \neq 0$, $r + 1 \geqslant s + u \geqslant 2$, 且若 $p = 2$ 则 $r \geqslant 2$.

K 仍如第二步所设. 当 $t = 0$ 时, 计算可得, 对于奇素数 p 有 $(ba^{-1})^{p^{r+s}} = 1$, 对于 $p = 2$ 有 $(ba^{2^u - 2^{r-1} - 1})^{2^{r+s}} = 1$. 用 ba^{-1} 或者 $ba^{2^u - 2^{r-1} - 1}$ 替换 b, 可得 (I) 型群.

以下设 $t \geqslant 1$. 当 $s = 0$ 时, 计算可得 $(a^{-1}b^{p^t})^{p^r} = 1$. 分别用 b 和 $a^{-1}b^{p^t}$ 去替换 a 和 b, 可得 (II) 型群. 当 $u = 0$ 以及 $su \neq 0$ 时, 易得 (III) 型群和 (IV) 型群.

第四步: 决定当 K 为直积因子时的群 G. 设 $G = K \times A$, 则易知 A 是非平凡的交换群.

此时, 若 K 是第三步中的 (I) 型群, 任取 $d \in A$ 并设 $o(d) = p^e$, 计算可知

$$[a^{p^{s+u-1}} d, b] = a^{p^{r+s+u-1}} \neq 1.$$

从而 $a^{p^r} \in \langle (a^{p^{s+u-1}} d)^{p^e} \rangle = \langle a^{p^{e+s+u-1}} \rangle$. 这说明 $e + s + u - 1 \leqslant r$, 从而有 $\exp A \leqslant p^{(r+1)-(s+u)}$. 因为 A 非平凡, 所以 $r + 1 > s + u$. 从而我们得到定理中的 (1) 型群.

若 K 是第三步中的 (II) 型群, 任取 $d \in A$ 并设 $o(d) = p^e$, 计算可知 $[a^{p^{u-1}} d, b] = a^{p^{r+t+u-1}} \neq 1$. 从而 $a^{p^{r+t}} \in \langle (a^{p^{u-1}} d)^{p^e} \rangle = \langle a^{p^{e+u-1}} \rangle$. 这说明 $e + u - 1 \leqslant r + t$, 从而有 $\exp A \leqslant p^{t+(r+1)-u}$. G 为定理中的 (2) 型群. 此时, G 还满足 $\exp A \leqslant p^r$.

若 K 是第三步中的 (III) 型群 (其中 $u = 0$) 或者 (IV) 型群, 任取 $d \in A$ 并设 $o(d) = p^e$, 计算可知 $[a^{p^{s+u-1}} d, b] = a^{p^{r+s+u-1}} \neq 1$. 从而 $a^{p^r} \in \langle (a^{p^{s+u-1}} d)^{p^e} \rangle = \langle a^{p^{e+s+u-1}} \rangle$. 这说明 $e + s + u - 1 \leqslant r$, 从而有 $\exp A \leqslant p^{(r+1)-(s+u)}$. 因为 A 非平凡, 所以 $r + 1 > s + u$. 从而我们得到定理中的 (3) 型群或者 (4) 型群.

第五步: 决定当 K 不是直积因子时的群 G. 设 $G = H \times A$, 其中 K 在 H 中无直积因子. 则易知 $K < H$ 且 A 是交换群.

由第二步, 可设 $H = K \rtimes B$, 其中 $B = \langle b_1\rangle \times \langle b_2\rangle \times \cdots \times \langle b_f\rangle$ 满足 $o(b_i) = p^{r_i}$, $r \geqslant r_1 \geqslant r_2 \geq \cdots \geqslant r_f$.

我们首先说明 K 不能是第三步中的 (III) 型群和 (IV) 型群. 若否, 通过计算可知 $\langle ab^{-p^t}\rangle) \cap \langle a\rangle = 1$. 因为子群 $\langle ab^{-p^t}, b_i\rangle$ 不包含 G', 所以由定理 6.1.3 有 $[ab^{-p^t}, b_i] = 1$. 同理有 $[b, b_i] = 1$, 从而 $H = K \times B$, 这与 H 的取法矛盾.

如果 K 是第三步中的 (I) 型群, 则一定有 $s = 0$. 若否, 通过计算可知 $\langle ab\rangle \cap \langle a\rangle \leqslant \langle a^{p^{r+1}}\rangle$. 因为子群 $\langle ab, b_i\rangle$ 不包含 G', 所以由定理 6.1.3 有 $[ab, b_i] = 1$. 同理有 $[b, b_i] = 1$, 从而 $H = K \times B$, 这与 H 的取法矛盾.

现在设 $K = \langle a, b\rangle$ 是第三步中 (II) 型群或 (I) 型群当 $s = 0$ 时的情形 (注意, 在 (II) 型群中让 t 可以取 0 就得到了 (I) 型群当 $s = 0$ 时的情形). 因为子群 $\langle b, b_i\rangle$ 不包含 G', 所以由定理 6.1.3 有 $[b, b_i] = 1$.

设 j 是使得 $[a, b_i]$ 的阶最大的最小的正整数. 我们总可不妨设 $j = 1$ (若 $j \neq 1$, 用 b_1b_j 来替换 b_1). 同理, 我们可不妨设 $\langle [a, b_1]\rangle \geqslant \langle [a, b_2]\rangle \geqslant \cdots \geqslant \langle [a, b_f]\rangle$.

设 $[a, b_i] = a^{\gamma_i p^{r+t_i}}$, 其中 $(\gamma_i, p) = 1$. 则 $t \leqslant t_1 \leqslant t_2 \leqslant \cdots \leqslant t_f$.

注意到 $a^b = a^{1+\gamma_i p^{r+t_i}}$. 由引理 7.3.4 和 7.3.5, 存在正整数 w 使得 $(1 + \gamma_i p^{r+t_i})^j \equiv 1 + p^{r+t_i} \pmod{p^{r+t+u}}$. 用 b_i^w 代替 b_i, 我们可不妨设 $[a, b_i] = a^{p^{r+t_i}}$. 则 $t \leqslant t_1 \leqslant t_2 \leqslant \cdots \leqslant t_f$. 以下我们分两种情况讨论:

情形 1: $t_1 > t$.

我们断言 $t_2 > t_1$: 若否, 则由 $[a, b_1b_2^{-1}] = 1$ 可知 $b_1b_2^{-1}$ 是 H 中 K 的直积因子, 矛盾. 同理我们有 $t < t_1 < t_2 < \cdots < t_f$. 由于 $[a, b_1b^{-p^{t_1-t}}] = 1$, 我们有 $(b_1b^{-p^{t_1-t}})^{p^{r_1}} \neq 1$ (若否, 则 $b_1b^{-p^{t_1-t}}$ 是 H 中 K 的直积因子, 矛盾). 从而我们有 $b^{p^{r_1+t_1-t}} \neq 1$, 即 $r_1 + t_1 - t < r$. 所以我们有 $r - r_1 > t_1 - t > 0$. 同理我们有 $r_i + t_i > r_{i+1} + t_{i+1}$. 由引理 7.3.4 和 7.3.5 可知, 在由 $\mathbb{Z}/p^{r+t+u}\mathbb{Z}$ 的可逆元组成的乘法群中, $1 + p^{r+t_f}$ 的阶是 p^{t+u-t_f}. 由 $[a, b_f^{p^{r_f}}] = 1$ 可知, $a^{b_f^{p^{r_f}}} = a^{(1+p^{r+t_f})^{p^{r_f}}} = a$. 所以我们还有 $r_f \geqslant t + u - t_f$, 即 $t_f + r_f \geqslant t + u$.

我们断言 $t_1 \geqslant u - 1$: 计算可得

$$\langle ba^{p^{t-t_1+u-1}}\rangle \cap \langle a\rangle = \langle (ba^{p^{t-t_1+u-1}})^{p^r}\rangle = \langle a^{p^{r+t-t_1+u-1}}\rangle.$$

考虑子群 $N = \langle ba^{p^{t-t_1+u-1}}, b_1\rangle$. 由于 $[ba^{p^{t-t_1+u-1}}, b_1] = a^{p^{r+t+u-1}} \neq 1$, 所以 N 非交换. 从而由定理 6.1.3 可知 $G' \leqslant N$. 这使得我们必有 $r + t - t_1 + u - 1 \leqslant r + t$, 即 $t_1 \geqslant u - 1$.

最后, 与第四步相同得到对 $\exp(A)$ 的限制, 就得到了定理中的 (5) 型群. 此时, G 还满足 $\exp A \leqslant p^r$.

情形 2: $t_1 = t$.

设 h 是使 $t_h = t$ 的最大的正整数, 则 $\langle a, b_h\rangle$ 是满足导群与 G' 相同的 G 的最小阶的子群, 且 $\langle a, b_h\rangle$ 满足以下定义关系:

$$a^{p^{r_h+t+(r-r_h)+u}} = 1, b_h^{p^{r_h}} = 1, a^{b_h} = a^{1+p^{r_h+t+(r-r_h)}}$$

我们令 $r' = r_h$, $t' = t + (r - r_h)$, 则以上关系可以写成:

$$a^{p^{r'+t'+u}} = 1, b_h^{p^{r'}} = 1, a^{b_h} = a^{1+p^{r'+t'}}$$

我们再令 $\tilde{K} = \langle a, b_h\rangle$, 并且分别用 $bb_h, b_1b_h^{-1}, \ldots, b_{h-1}b_h^{-1}$ 替换 $b, b_1, \ldots, b_{h_1}$, 则我们可不妨设 $b, b_1, \ldots, b_{h-1}$ 都是 G 的直积因子. 此时, 我们用 $A \times \langle b\rangle \times \langle b_1\rangle \times \cdots \times \langle b_{h-1}\rangle$ 来替换原来的 A.

若 $h = f$, 则 $G = \tilde{K} \times A$. 此时, 与第四步相同可以得到 $\exp A \leqslant p^{t'+(r'+1)-u}$. 因此, 我们得到了定理中的 (2) 型群当 $\exp(A) > p^r$ 的情形.

若 $h < f$, 我们令 $f' = f - h$. 对于 $1 \leqslant i \leqslant f'$, 我们令 $b'_i = b_{h+i}$, $t'_i = t_{h+i}$. 再令 $\tilde{B} = \langle b'_1\rangle \times \ldots \langle b'_{f'}\rangle$, $\tilde{H} = \tilde{K} \rtimes \tilde{B}$. 则 $\tilde{K}$ 在 $\tilde{H}$ 中无直积因子. 此时, 一定有 $t'_1 > t'$. 除了 $\exp(A) > p^{r'}$ 外, 与情形 1 完全相同. 最后, 我们可以得到定理中的 (5) 型群当 $\exp A > p^r$ 的情形. □

定理 7.3.7. 设 p 为奇素数, $G = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1+m_2}} = a_2^{p^{m_2+1}} = a_3^p = 1, [a_1, a_2] = a_1^{p^{m_1}}, [a_1, a_3] = a_2^{p^{m_2}}, [a_2, a_3] = 1\rangle$, 其中 $m_1 > m_2 \geqslant 1$. 则 $c(G) = 3$, $G' = \langle a_1^{p^{m_1}}\rangle \times \langle a_2^{p^{m_2}}\rangle$, $G_3 = \langle a_1^{p^{m_1+m_2}}\rangle$, $Z(G) = \langle a_1^{p^{m_2+1}}\rangle$. G 是有限亚 *Hamilton* p 群. 不同的参数对应的群互不同构.

证明 首先, 由 $[a_1, a_2] = a_1^{p^{m_1}}$ 可得

$$a_1^{a_2} = a_1^{1+p^{m_1}}.$$

由引理 7.3.4 可知, 在由 $\mathbb{Z}/p^{m_1+1+m_2}\mathbb{Z}$ 的可逆元组成的乘法群中, $1 + p^{m_1}$ 的阶是 p^{m_2+1}. 所以 $a_1^{(1+p^{m_1})^{p^{m_2+1}}} = a_1^{a_2^{p^{m_2+1}}} = a_1$, 从而 a_2 在 $\langle a_1\rangle$ 上诱导了一个 p^{m_2+1} 阶自同构. 由群的扩展理论可知 $\langle a_1\rangle \rtimes \langle a_2\rangle$ 是一个良定义的亚循环群.

又由 $[a_1,a_3]=a_2^{p^{m_2}},[a_2,a_3]=1$ 可得 $a_1^{a_3}=a_1a_2^{p^{m_2}},a_2^{a_3}=a_2$. 计算可知 a_3 在 $\langle a_1,a_2\rangle$ 上诱导了一个 p 阶的自同构. 由群的扩展理论可知定理中所给的群是良定义的.

易知 $\langle a_1^{p^{m_1}},a_2^{p^{m_2}}\rangle\trianglelefteq G$, 并且 $G/\langle a_1^{p^{m_1}},a_2^{p^{m_2}}\rangle$ 交换. 所以 $G'\leqslant\langle a_1^{p^{m_1}},a_2^{p^{m_2}}\rangle$, 且进一步有 $G'=\langle a_1^{p^{m_1}},a_2^{p^{m_2}}\rangle$.

计算可得 $[a_1,a_2^{p^{m_2}}]=a_1^{p^{m_1+m_2}}$, $[a_1^{p^{m_1}},a_2]=a_1^{p^{m_1+m_1}}\in\langle a_1^{p^{m_1+m_2}}\rangle\leqslant Z(G)$. 所以 $c(G)$=3 且 $G_3=\langle a_1^{p^{m_1+m_2}}\rangle$.

任取 G 的元素 $b=a_3^ia_2^ja_1^k$, 若 $p\nmid i$ 或者 $p^{m_2+1}\nmid j$, 则 $[b,a_1]\neq1$. 所以 $Z(G)\leqslant\langle a_1\rangle$. 又因为 $[a_1^p,a_3]=1$, $[a_1^{p^{m_2+1}},a_2]=1$, 所以 $Z(G)=\langle a_1^{p^{m_2+1}}\rangle$.

由 G/G' 的型不变量为 (p^{m_1},p^{m_2},p) 可知, 不同的参数对应的群互不同构.

最后我们来证明 G 一定是有限亚 Hamilton p 群. 考虑它的二元生成的子群 H. 注意到 $\langle a_1^p,a_2\rangle\times a_3$ 是 G 的极大子群, 我们可设 $H=\langle\rho_1,\rho_2\rangle$, 其中 $\rho_1=a_1^ia_2^{i_2}a_3^{i_3}a_1^{i_1p}$, $\rho_2=a_2^{j_2}a_3^{j_3}a_1^{j_1p}$, $0\leqslant i\leqslant(p-1)$.

若 $i=0$, 不妨设 $a_2^{j_2}\in\langle a_2^{i_2}\rangle$. 设 $a_2^{j_2}=(a_2^{i_2})^k$, 则 $\rho_1^{-k}\rho_2\in\langle a_1^p,a_3\rangle$. 所以, 我们可不妨设 $\rho_1=a_2^{p^\alpha}a_3^sa_1^{tp},\rho_2=a_3^ua_1^{vp^{\beta+1}}$, 其中 $(v,p)=1$. 考虑 ρ_2^p 可知 $a_1^{p^{\beta+2}}\in H$. 又因为 $\rho_1^{p^{\beta+1}}\equiv a_2^{p^{\alpha+\beta+1}}\pmod{\langle a_1^{tp^{\beta+2}}\rangle}$, 所以又有 $a_2^{p^{\alpha+\beta+1}}\in H$. 此时, 若 $\alpha+\beta<m_2$, 则有 $\alpha+\beta+1\leqslant m_2$ 且 $\beta+2\leqslant m_2-\alpha+1\leqslant m_2+1\leqslant m_1$, 从而 $G'\leqslant H$, $H\trianglelefteq G$; 若 $\alpha+\beta\geqslant m_2$, 则 $[\rho_1,\rho_2]=[a_2^{p^\alpha},a_1^{vp^{\beta+1}}]=1$, 从而 H 交换.

若 $i\neq0$, 我们可不妨设 $i=1$. 此时, 由于 $m_1>m_2$, 计算可得 $\langle\rho_1^{p^{m_1}}\rangle=\langle a_1^{p^{m_1}}\rangle$. 因为 $\langle\rho_1^p,a_2\rangle\times a_3$ 也是 G 的极大子群, 所以我们可不妨设 $\rho_2=a_2^{j_2}a_3^{j_3}\rho_1^{j_1p}$. 此时, 若 $(p,j_3)=1$, 则 $[\rho_1,\rho_2]\equiv[a_1,a_3^{j_3}]\equiv a_2^{j_3p^{m_2}}\pmod{\langle a_1^{p^{m_1}}\rangle}$, 因此 $G'\leqslant H$, $H\trianglelefteq G$; 若 $p\mid j_3$, 则 $H=\langle\rho_1,a_2^{j_2}\rangle$, 也有 $H\trianglelefteq G$.

因为以上讨论了 G 的所有二元生成子群, 所以由定理 6.1.1 可知 G 一定是有限亚 Hamilton p 群. □

定理 7.3.8. 设 $G=K\times A$, 其中 $K=\langle a_1,a_2,a_3\mid a_1^{p^{m_1+1+k}}=a_2^{p^{m_2+1}}=a_3^{p^{m_3}}=1,[a_1,a_2]=a_1^{p^{m_1}},[a_1,a_3]=a_2^{p^{m_2}},[a_2,a_3]=1\rangle$, 其中 $m_1\geqslant m_2\geqslant m_3$, $1\leqslant k\leqslant\min\{m_1-m_3,m_2-m_3+1,m_2-1\}$. A 是满足 $\exp(A)\leqslant p^{m_2-k}$ 的交换群. 则 $c(G)=2$, $G'=\langle a_1^{p^{m_1}}\rangle\times\langle a_2^{p^{m_2}}\rangle$, $Z(G)=\langle a_1^{p^{k+1}}\rangle\times\langle a_2^{p^{k+1}}\rangle\times\langle a_3^p\rangle\times A$. G 是有限亚 *Hamilton* p 群, 不同的参数或者不同的交换群 A 对应的群互不同

构.

证明 首先, 由 $1 \leqslant k \leqslant m_2 - 1$ 可得 $m_1 \geqslant m_2 \geqslant 2$. 由 $[a_1, a_2] = a_1^{p^{m_1}}$ 可得 $a_1^{a_2} = a_1^{1+p^{m_1}}$. 由引理 7.3.4 和引理 7.3.5 可知, 在由 $\mathbb{Z}/p^{m_1+1+k}\mathbb{Z}$ 的可逆元组成的乘法群中, $1 + p^{m_1}$ 的阶是 p^{k+1}. 所以 $a_1^{a_2^{p^{k+1}}} = a_1^{(1+p^{m_1})^{p^{k+1}}} = a_1$, 从而 a_2 在 $\langle a_1 \rangle$ 上诱导了一个 p^{k+1} 阶自同构. 由群的扩展理论可知 $\langle a_1 \rangle \rtimes \langle a_2 \rangle$ 是一个良定义的亚循环群. 并且我们还知道 $[a_1, a_2^{p^k}] \neq 1$ 和 $[a_1, a_2^{p^{k+1}}] = 1$. 又由 $[a_1, a_3] = a_2^{p^{m_2}}, [a_2, a_3] = 1$ 可得 $a_1^{a_3} = a_1 a_2^{p^{m_2}}, a_2^{a_3} = a_2$. 计算可知 a_3 在 $\langle a_1, a_2 \rangle$ 上诱导了一个 p 阶的自同构. 由群的扩展理论可知定理中所给的群是良定义的.

任取 G 的元素 $b = a_3^i a_2^j a_1^k$. 若 $p \nmid i$ 或者 $p^{k+1} \nmid j$, 则 $[b, a_1] \neq 1$; 若 $p^{k+1} \nmid j$, 则 $[b, a_2] \neq 1$. 所以 $Z(G) = \langle a_1^{p^{k+1}}, a_2^{p^{k+1}}, a_3^p \rangle$.

因为 $G' = \langle a_1^{p^{m_1}}, a_2^{p^{m_2}} \rangle \leqslant Z(G)$, 所以 $c(G) = 2$.

由于 G' 的型不变量为 (p^{k+1}, p), 所以 k 是 G 的不变量. 又因为 $G/\mho_1(G')$ 为定理 7.1.2 中的 (II) 型群, 所以 m_1, m_2, m_3 也是 G 的不变量, 并且不同构的 A 对应的群互不同构.

最后我们来证明 G 一定是有限亚 Hamilton p 群. 考虑它的二元生成的子群 H. 注意到 $\langle a_1^p, a_2 \rangle \times a_3 \times A$ 是 G 的极大子群, 我们可设 $H = \langle \rho_1, \rho_2 \rangle$, 其中 $\rho_1 = a_1^i a_2^{i_2} a_3^{i_3} a_1^{i_1 p} x$, $\rho_2 = a_2^{j_2} a_3^{j_3} a_1^{j_1 p} y$, 其中 $0 \leqslant i \leqslant (p-1)$, $x, y \in A$.

若 $i = 0$, 不妨设 $a_2^{j_2} \in \langle a_2^{i_2} \rangle$. 设 $a_2^{j_2} = (a_2^{i_2})^k$, 则 $\rho_1^{-k}\rho_2 \in \langle a_1^p, a_3, A \rangle$. 所以, 我们可不妨设 $\rho_1 = a_2^{p^\alpha} a_3^s a_1^{tp} x, \rho_2 = a_3^u a_1^{p^{\beta+1}} y$, 其中 $x, y \in A$. 此时, 若 $\alpha + \beta \geqslant k$, 则 $[\rho_1, \rho_2] = [a_2^{p^\alpha}, a_1^{p^{\beta+1}}] = 1$, 从而 H 交换; 若 $\alpha + \beta \leqslant k - 1$, 则有 $m_1 - \beta - 1 \geqslant m_1 - k \geqslant \max\{m_3, m_2 - k\}$, 从而 $a_1^{p^{m_1}} = \rho_2^{p^{m_1-\beta-1}} \in H$. 又因为 $m_2 - (\alpha + \beta) \geqslant m_2 - k + 1 \geqslant \max\{m_3, \exp(A)\}$, 所以 $(\rho_1^{p^\beta} \rho_2^{-t})^{p^{m_2-(\alpha+\beta)}} \equiv a_2^{p^{m_2}} \pmod{\langle a_1^{p^{m_1}} \rangle}$, 从而 $G' \leqslant H$, $H \trianglelefteq G$.

若 $i \neq 0$, 我们可不妨设 $i = 1$. 因为

$$\langle \rho_1^p, a_2 \rangle \times a_3 \times A$$

也是 G 的极大子群. 所以我们可不妨设 $\rho_2 = a_2^{j_2} a_3^{j_3} \rho_1^{j_1 p} a_1^{j p^{m_1}} y$, 其中 $y \in A$. 因为 $\rho_2 \rho_1^{-j_1 p} \in \langle a_2, a_3, a_1^{j p^{m_1}}, A \rangle$, 进一步可不妨设 $\rho_2 = a_2^{p^\alpha} a_3^{j_3} a_1^{j p^{m_1}} y$, 其中 $\alpha \geqslant 0$, $y \in A$. 此时, 若 $\alpha = 0$, 则 $a_2^{p^{m_2}} = \rho_2^{p^{m_2}} \in H$, 进一步, 因为 $a_1^{p^{m_1}} \equiv$

$\rho_1^{p^{m_1}} \pmod{\langle a_2^{p^{m_2}}, a_1^{p^{m_1+1}}\rangle}$, 所以 $G' \leqslant H$, 从而 $H \trianglelefteq G$; 若 $\alpha \geqslant 1$ 且 $(j_3, p) = 1$, 则 $[\rho_1, \rho_2] \equiv [a_1, a_3^{j_3}] \equiv a_2^{j_3 p^{m_2}} \pmod{\langle a_1^{p^{m_1+1}}\rangle}$, 进一步, 因为 $a_1^{p^{m_1}} \equiv \rho_1^{p^{m_1}} \pmod{\langle a_2^{p^{m_2}}, a_1^{p^{m_1+1}}\rangle}$, 所以 $G' \leqslant H$, 从而 $H \trianglelefteq G$; 若 $\alpha \geqslant k+1$ 且 $p \mid j_3$, 则 H 交换; 最后, 若 $1 \leqslant \alpha \leqslant k$ 且 $p \mid j_3$, 由 $m_2 - \alpha \geqslant m_2 - k \geqslant \max\{m_3 - 1, 1\}$ 可得 $a_2^{p^{m_2}} \equiv \rho_2^{p^{m_2-\alpha}} \pmod{\langle a_1^{p^{m_1+1}}\rangle}$, 进一步, 因为 $a_1^{p^{m_1}} \equiv \rho_1^{p^{m_1}} \pmod{\langle a_2^{p^{m_2}}, a_1^{p^{m_1+1}}\rangle}$, 所以 $G' \leqslant H$, 从而 $H \trianglelefteq G$.

因为以上讨论了 G 的所有二元生成子群, 所以由定理 6.1.1 可知 G 一定是有限亚 Hamilton p 群. □

定理 7.3.9. *设 G 是有限亚 Hamilton p 群. 若 $\exp(G') > p$ 且 G' 非循环, 则 G 定理 7.3.7 或者定理 7.3.8 中的群. 即以下两种类型:*

(1) $G = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1+m_2}} = a_2^{p^{m_2+1}} = a_3^p = 1, [a_1, a_2] = a_1^{p^{m_1}}, [a_1, a_3] = a_2^{p^{m_2}}, [a_2, a_3] = 1\rangle$, 其中 $m_1 > m_2 \geqslant 1$, p 为奇素数.

(2) $G = K \times A$. 其中 $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1+k}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3}} = 1, [a_1, a_2] = a_1^{p^{m_1}}, [a_1, a_3] = a_2^{p^{m_2}}, [a_2, a_3] = 1\rangle$. 其中 $m_1 \geqslant m_2 \geqslant m_3$, $1 \leqslant k \leqslant \min\{m_1 - m_3, m_2 - m_3 + 1, m_2 - 1\}$. A 是满足 $\exp(A) \leqslant p^{m_2-k}$ 的交换群.

证明　设 H 为 G 的二元生成的子群, 满足 $\exp(H') > p$. 由定理 7.3.3 可知 H 为亚循环的. 又由定理 6.1.3 可知 $G' < H$, 从而 G' 也是亚循环的.

令 $N = \mho_1(G')$, $\bar{G} = G/N$, 则 $\bar{G}'$ 为 p^2 阶的初等交换群. 由定理 7.3.3 可知 $d(G) > 2$, 从而 $d(\bar{G}) > 2$. 再由推论 6.2.4 可知, $c(\bar{G}) = 2$. 从而 $\bar{G}$ 只能是定理 7.1.4 中的群.

若 $\bar{G}$ 是定理 7.1.4 中的 (1) 型群. 设 $\bar{G} = \bar{K} \times \bar{A}$. 其中 $\bar{K} = \langle \bar{a}_1, \bar{a}_2, \bar{a}_3 \mid \bar{a}_1^{p^{m_1}} = \bar{a}_2^{p^{m_2+1}} = \bar{a}_3^{p^{m_3+1}} = 1, [\bar{a}_1, \bar{a}_2] = \bar{a}_3^{p^{m_3}}, [\bar{a}_1, \bar{a}_3] = \bar{a}_2^{p^{m_2}}, [\bar{a}_2, \bar{a}_3] = 1\rangle$, $m_1 \geqslant m_2 = m_3 + 1$, $\bar{A}$ 是满足 $\exp(\bar{A}) \leqslant p^{m_3}$ 的交换群. 则

$$G' = \langle [a_1, a_2], [a_1, a_3], \mho_1(G')\rangle = \langle [a_1, a_2], [a_1, a_3]\rangle = \langle a_2^{p^{m_2}}, a_3^{p^{m_3}}\rangle.$$

由于 $\langle \bar{a}_1, \bar{a}_2\rangle$ 和 $\langle \bar{a}_1, \bar{a}_3\rangle$ 都非亚循环, 所以 $\langle a_1, a_2\rangle$ 和 $\langle a_1, a_3\rangle$ 也非亚循环. 从而由定理 7.3.3 可知 $[a_1, a_2]$ 和 $[a_1, a_3]$ 都是 p 阶元. 进一步, $\exp(G') = p$, 与题设矛盾.

同理可知 $\bar{G}$ 也不可能是定理 7.1.4 中的 (2) 型群, (3) 型群以及 (6), (7), (8) 型群.

若 $\bar{G}$ 是定理 7.1.4 中的 (5) 型群. 设 $\bar{G}=\bar{K}\times\bar{A}$. 其中 $\bar{K}=\langle\bar{a}_1,\bar{a}_2,\bar{a}_3\mid\bar{a}_1^{p^{m_1+1}}=\bar{a}_2^{p^{m_2}}=\bar{a}_3^{p^{m_3+1}}=1,[\bar{a}_1,\bar{a}_2]=\bar{a}_3^{p^{m_3}},[\bar{a}_1,\bar{a}_3]=\bar{a}_1^{p^{m_1}},[\bar{a}_2,\bar{a}_3]=1\rangle$, $m_1\geqslant m_2=m_3+1$, $\bar{A}$ 是满足 $\exp(\bar{A})\leqslant p^{m_3}$ 的交换群. 则

$$G'=\langle[a_1,a_2],[a_1,a_2a_3],$$

$$\mho_1(G')\rangle=\langle[a_1,a_2],[a_1,a_2a_3]\rangle=\langle a_1^{p^{m_1}},a_3^{p^{m_3}}\rangle.$$

由于 $\langle\bar{a}_1,\bar{a}_2\rangle$ 和 $\langle\bar{a}_1,\bar{a}_2\bar{a}_3\rangle$ 都非亚循环, 所以 $\langle a_1,a_2\rangle$ 和 $\langle a_1,a_2a_3\rangle$ 也非亚循环. 从而由定理 7.3.3 可知 $[a_1,a_2]$ 和 $[a_1,a_2a_3]$ 都是 p 阶元. 进一步, $\exp(G')=p$, 与题设矛盾.

若 $\bar{G}$ 是定理 7.1.4 中的 (9) 型群. 设 $\bar{G}=\bar{K}\times\bar{A}$. 其中 $K=\langle\bar{a}_1,\bar{a}_2,\bar{b}\mid\bar{a}_1^4=\bar{a}_2^4=1,\bar{b}^2=\bar{a}_1^2,[\bar{a}_1,\bar{a}_2]=1,[\bar{a}_1,\bar{b}]=\bar{a}_2^2,[\bar{a}_2,\bar{b}]=\bar{a}_1^2\rangle$, $\bar{A}$ 是满足 $\exp(\bar{A})\leqslant 2$ 的交换群. 则 $G'=\langle[a_1,b],[a_2,b],\mho_1(G')\rangle=\langle a_1^2,a_2^2\rangle$, $\mho_1(G')=\langle a_1^4,a_2^4\rangle$, $\mho_2(G')=\langle a_1^4,a_2^4\rangle$. 设 M 是在 G 中正规的 $\mho_1(G')$ 的极大子群, 并设 $M=\langle e,\mho_2(G')\rangle$, 则 $e\in C_G(G/M)$. 由 $G/\mho_1(G')$ 的表示可设 $[a_1,a_2]\equiv e^i\pmod M$. 从而 $[a_1^2,a_2]\equiv[a_1,a_2^2]\equiv 1\pmod M$. 还是由 $G/\mho_1(G)$ 的表示可设 $b^2\equiv a_1^2e^j\pmod M$. 从而

$$[a_1^2,b]\equiv[a_1,b^2]\equiv 1\pmod M \tag{1}$$

再设 $[a_1,b]\equiv a_2^2e^k\pmod M$ 用命题 1.1.1 计算可得:

$$[a_1^2,b]\equiv[a_1,b]^2[a_1,b,a_1]\equiv a_2^4\pmod M \tag{2}$$

由 (1), (2) 得 $a_2^4\in M$, 从而 $M=\langle a_1^8,a_2^4\rangle$. 我们再考虑 G/M 的子群 $\langle a_1M,bM\rangle$, 由于它的导群为初等交换 2 群, 由定理 6.2.1 可知它的幂零类为 2, 从而

$$[a_2^2,b]\equiv 1\pmod M \tag{3}$$

再用命题 1.1.1 计算可得:

$$[a_2^2,b]\equiv[a_2,b]^2[a_2,b,a_2]\equiv a_1^4\pmod M \tag{4}$$

由 (3), (4) 得 $a_1^4\in M$, 从而 $M=\mho_1(G)$, 矛盾.

注意到 (10) 型群是一个 (9) 型群的二次扩张, 同理可知 $\bar{G}$ 不能与定理 7.1.4 中的 (10) 型群同构.

最后, $\bar{G}$ 只能与定理 7.1.4 中的 (4) 型群同构. 设 $\bar{G} = \bar{K} \times \bar{A}$, 其中 $\bar{K} = \langle \bar{a_1}, \bar{a_2}, \bar{a_3} \mid \bar{a_1}^{p^{m_1+1}} = \bar{a_2}^{p^{m_2+1}} = \bar{a_3}^{p^{m_3}} = 1, [\bar{a_1}, \bar{a_2}] = \bar{a_1}^{p^{m_1}}, [\bar{a_1}, \bar{a_3}] = \bar{a_2}^{p^{m_2}}, [\bar{a_2}, \bar{a_3}] = 1 \rangle$, 其中 $m_1 \geqslant m_2 \geqslant m_3$. 若 $p=2$, 则 $m_1 > 1$. $\bar{A}$ 是满足 $\exp(\bar{A}) \leqslant p^{m_2}$ 的交换群; 则 $G' = \langle a_1^{p^{m_1}}, a_2^{p^{m_2}} \rangle$.

由于 $\langle \bar{a}_2, \bar{a}_3 \rangle$ 不包含 G', 所以 $\langle a_2, a_3 \rangle$ 也不包含 G'. 这说明 $[a_2, a_3] = 1$. 同理, $\langle a_2, a_3 a_1^{p^{m_1}} \rangle$ 也不包含 G', 从而 $[a_2, a_3 a_1^{p^{m_1}}] = 1$, 进而有 $[a_1^{p^{m_1}}, a_2] = a_1^{p^{2m_1}} = 1$. 设 a_1 的阶为 p^{m_1+1+k}, 其中 $k \geqslant 1$, 则我们有 $m_1 > k$.

设 $\bar{A} = \langle \bar{a}_4 \rangle \times \langle \bar{a}_5 \rangle \times \cdots \times \langle \bar{a}_f \rangle$, 其型不变量为 $(p^{m_4}, p^{m_5}, \dots, p^{m_f})$. 对于 $4 \leqslant i \leq f$ 和 $1 \leqslant j \leqslant f$, 由于 $\langle \bar{a}_i, \bar{a}_j \rangle$ 不包含 G', 所以 $\langle a_i, a_j \rangle$ 也不包含 G'. 这说明 $[a_i, a_j] = 1$, 从而 $a_i \in Z(G)$. 设 $a_i^{p^{m_i}} = a_1^{sp^{m_1+1}}$, 则 $(a_i a_1^{-sp^{m_1+1-m_i}})^{p^{m_i}} = 1$. 令 $b_i = a_i a_1^{-sp^{m_1+1-m_i}}$, $A = \langle b_4 \rangle \times \langle b_5 \rangle \times \cdots \times \langle b_f \rangle$, 并设 $K = \langle a_1, a_2, a_3 \rangle$, 则 $G = K \times A$.

设 $[a_1, a_2] = a_1^{p^{m_1}} a_1^{up^{m_1+1}}$, 即 $a_1^{a_2} = a_1^{1+(1+up)p^{m_1}}$. 由引理 7.3.4 和引理 7.3.5, 存在正整数 w 使得 $(1+(1+up)p^{m_1})^j = 1 + p^{m_1}$. 分别用 a_2^w 和 a_3^w 代替 a_2 和 a_3, 我们可不妨设 $[a_1, a_2] = a^{p^{m_1}}$.

由于 $\langle \bar{a}_1, a_3 \rangle$ 非亚循环, 所以 $\langle a_1, a_3 \rangle$ 也非亚循环. 由定理 7.3.3 可知 $[a_1, a_3]^p = 1$. 设 $[a_1, a_3] = a_2^{p^{m_2}} d$, 其中 $d \in \mho_1(G')$, 则 $a_2^{p^{m_2+1}} d^p = 1$. 这说明 $a_2^{p^{m_2+1}} \in \mho_2(G')$, 从而 $N = \mho_1(G') = \langle a_1^{p^{m_1+1}}, a_2^{p^{m_2+1}} \rangle = \langle a_1^{p^{m_1+1}} \rangle$, $a_2^{p^{m_2+1}} \in \langle a_1^{p^{m_1+2}} \rangle$.

由引理 7.3.4 和引理 7.3.5 可知, 在由 $\mathbb{Z}/p^{m_1+1+k}\mathbb{Z}$ 的可逆元组成的乘法群中, $1+p^{m_1}$ 的阶是 p^{k+1}. 由于 $a_1^{(1+p^{m_1})^{p^{m_2+1}}} = a_1^{a_2^{p^{m_2+1}}} = a_1$, 所以我们有 $k+1 \leqslant m_2+1$, 即 $k \leqslant m_2$. 以下我们分两种情形讨论:

情形 1: $k = m_2$. 此时, $[a_1, a_2^{p^{m_2}}] \neq 1$ 并且有 $m_1 > m_2$.

这时, 由于 $\langle a_1, a_3 \rangle$ 的幂零类大于 2, 由推论 6.2.4 可知, p 为奇素数且 $\langle a_1, a_3 \rangle$ 为 $\mathcal{A}_2$ 群. 若 $m_3 > 1$, 则有子群 $\langle a_1, a_2^{p^{m_2}} a_3^p \rangle$ 既不交换也不正规. 所以, 一定有 $m_3 = 1$. 若 $A \neq 1$, 则对任意的 $1 \neq e \in A$, 我们有子群 $\langle a_1, a_2^{p^{m_2}} e \rangle$ 既不交换也不正规. 所以, 一定有 $A = 1$. 设 $a_3^p = a_1^{vp^{m_1+1}}$, 则 $(a_3 a_1^{-vp^{m_1}})^p = 1$. 用 $a_3 a_1^{-vp^{m_1}}$ 来替换 a_3, 我们可不妨设 $a_3^p = 1$.

设 $[a_1,a_3]=a_2^{p^{m_2}}a_1^{wp^{m_1+1}}$, 即 $a_2^{p^{m_2+1}}a_1^{wp^{m_1+2}}=1$. 注意到 G 是 p^{m_2+1} 交换的, 我们有 $(a_2a_1^{wp^{m_1-m_2+1}})^{p^{m_2+1}}=1$. 再设

$$(a_2a_1^{wp^{m_1-m_2+1}})^{p^{m_2}}=a_2^{p^{m_2+1}}a_1^{wp^{m_1+2}}a_1^{xp^{m_1+m_2}},$$

则

$$(a_2a_1^{wp^{m_1-m_2+1}}a_1^{-xp^{m_1}})^{p^{m_2}}=a_2^{p^{m_2}}a_1^{wp^{m_1+1}}=[a_1,a_3].$$

用 $a_2a_1^{wp^{m_1-m_2+1}}a_1^{-xp^{m_1}}$ 来替换 a_2, 我们可不妨设 $a_2^{p^{m_2+1}}=1$ 并且 $[a_1,a_3]=a_2^{p^{m_2}}$.

在这种情形下, 我们得到了定理中的 (1) 型群.

情形 2: $k<m_2$. 此时 $[a_1,a_2^{p^{m_2}}]=1$.

由于 $[a_1,a_3,a_1]=1$, 我们有 $[a_1^p,a_3]=[a_1,a_3]^p=1$, 从而 $\langle a_1^p,a_2\rangle$ 与 a_3 交换. 这时 $\langle a_1,a_3\rangle$ 是内交换群. 由于 $\langle a_2,a_3a_1^{p^{m_1-m_3+1}}\rangle$ 不包含 G', 我们有 $[a_2,a_3a_1^{p^{m_1-m_3+1}}]=1$. 进而我们有 $1=[a_1^{p^{m_1-m_3+1}},a_2]=a_1^{p^{2m_1-m_3+1}}$, 从而 $2m_1-m_3+1\geqslant m_1+1+k$, 即 $m_1-m_3\geqslant k$. 由于 $\langle a_1,a_2^{p^{m_2-m_3+2}}a_3^p\rangle$ 不包含 G', 我们有 $[a_1,a_2^{p^{m_2-m_3+2}}a_3^p]=1$, 进而我们有 $a_1^{a_2^{p^{m_2-m_3+2}}}=a_1^{(1+p^{m_1})^{p^{m_2-m_3+2}}}=a_1$. 由于在由 $\mathbb{Z}/p^{m_1+1+k}\mathbb{Z}$ 的可逆元组成的乘法群中, $1+p^{m_1}$ 的阶是 p^{k+1}, 所以我们有 $m_2-m_3+2\geqslant k+1$, 即 $k\leqslant m_2-m_3+1$.

对任意的 $b\in A$, 设 b 的阶为 p^e. 由于 $\langle a_1,a_2^{p^{m_2-e+1}}b\rangle$ 不包含 G', 我们有

$$[a_1,a_2^{p^{m_2-e+1}}b]=1.$$

进而我们有 $a_1^{a_2^{p^{m_2-e+1}}}=a_1^{(1+p^{m_1})^{p^{m_2-e+1}}}=a_1$. 由于在由 $\mathbb{Z}/p^{m_1+1+k}\mathbb{Z}$ 的可逆元组成的乘法群中, $1+p^{m_1}$ 的阶是 p^{k+1}, 所以我们有 $m_2-e+1\geqslant k+1$, 即 $e\leqslant m_2-k$. 由 b 的任意性有 $\exp(A)\leqslant p^{m_2-k}$.

设 $a_3^p=a_1^{vp^{m_1+1}}$, 则 $(a_3a_1^{-vp^{m_1}})^p=1$. 用 $a_3a_1^{-vp^{m_1}}$ 来替换 a_3, 我们可不妨设 $a_3^p=1$.

设 $[a_1,a_3]=a_2^{p^{m_2}}a_1^{wp^{m_1+1}}$, 即 $a_2^{p^{m_2+1}}a_1^{wp^{m_1+2}}=1$. 注意到 $c(G)=2$, 我们有

$$(a_2a_1^{wp^{m_1-m_2+1}})^{p^{m_2}}=a_2^{p^{m_2}}a_1^{wp^{m_1+1}}.$$

用 $a_2a_1^{wp^{m_1-m_2+1}}$ 来替换 a_2, 我们可不妨设 $a_2^{p^{m_2+1}}=1$ 并且 $[a_1,a_3]=a_2^{p^{m_2}}$.

在这种情形下, 我们得到了定理中的 (2) 型群.

最后, 因为两种类型的群幂零类不同, 所以它们互不同构. □

§7.4 小结

下面是有限亚 Hamilton p 群的完全分类:

定理 7.4.1. *设 G 是有限 p 群, 则 G 是亚 Hamilton 群当且仅当 G 是以下互不同构的群之一:*

类型 (I): $|G'| = p$ 的有限 p 群 (分类见文献 [20]);

类型 (II): $\exp(G') = p$ 且 $c(G) = 3$. 此时, G 一定为 $\mathcal{A}_2$ 群, $d(G) = 2$ 且 p 为奇素数. 即以下几种群:

(1) *p^4 阶的极大类 p 群:*

(i) $\langle a, b, c, d \mid a^p = b^p = c^p = d^p = 1, [c, d] = b, [b, d] = a, [a, b] = [a, c] = [a, d] = [b, c] = 1\rangle$;

(ii) $\langle a, b, c \mid a^{p^2} = b^p = 1, c^p = a^{\alpha p}, [a, b] = a^p, [a, c] = b, [b, c] = 1\rangle$, 其中 $\alpha = 0, 1$ 或是一个模 p 的平方非剩余 (三种互不同构的群);

(iii) $p = 3$, $\langle a, b, c \mid a^9 = b^3 = c^3 = 1, [a, b] = 1, [a, c] = b, [c, b^{-1}] = a^{-3}\rangle$.

(2) *二元生成有交换极大子群的 $\mathcal{A}_2$ 群 ($n \geqslant 5$):*

(i) $\langle b, a_1, a_2, a_3 \mid b^{p^{n-3}} = a_1^p = a_2^p = a_3^p = 1, [a_1, b] = a_2, [a_2, b] = a_3, [a_i, a_j] = 1, [a_3, b] = 1\rangle$, 其中 $1 \leqslant i, j \leqslant 3$;

(ii) $\langle b, a_1, a_2 \mid b^{p^{n-2}} = a_1^p = a_2^p = 1, [a_1, b] = a_2, [a_2, b] = b^{p^{n-3}}, [a_1, a_2] = 1, [b^{p^{n-3}}, a_1] = [b^{p^{n-3}}, a_2] = 1\rangle$;

(iii) $\langle b, a_1, a_2 \mid b^{p^{n-3}} = a_1^{p^2} = a_2^p = 1, [a_1, b] = a_2, [a_2, b] = a_1^{\nu p}, [a_1, a_2] = 1, [a_1^p, b] = [a_1^p, a_2] = 1\rangle$, 其中 $\nu = 1$ 或者 ν 是一个固定的模 p 的平方非剩余.

(3) *无交换极大子群的 $\mathcal{A}_2$ 群 ($p \geqslant 5$):*

(i) $\langle a, b \mid a^{p^2} = b^{p^2} = c^p = 1, [a, b] = c, [c, a] = b^{\nu p}, [c, b] = a^p\rangle$, 其中 ν 是固定的模 p 的平方非剩余;

(ii) $\langle a, b \mid a^{p^2} = b^{p^2} = c^p = 1, [a, b] = c, [c, a] = a^{-p}b^{-lp}, [c, b] = a^{-p}\rangle$, 其中 $4l = g^{2r+1} - 1$ 对于 $r = 1, 2, \ldots, \frac{1}{2}(p-1)$, g 是模 p

的最小原根;

(4) 无交换极大子群的 $\mathcal{A}_2$ 群 $(p=3)$:

(i) $\langle a,b \mid a^9=b^9=c^3=1,[a,b]=c,[c,a]=b^{-3},[c,b]=a^3\rangle$;

(ii) $\langle a,b \mid a^9=b^9=c^3=1,[a,b]=c,[c,a]=b^{-3},[c,b]=a^{-3}\rangle$.

类型 (III): $c(G)=2$ 且 G' 为 p^2 阶初等交换群. G 有以下几种互不同构的类型:

(1) $G=K\times A$. 其中 $K=\langle a_1,a_2,a_3 \mid a_1^{p^{m_1}}=a_2^{p^{m_2+1}}=a_3^{p^{m_3+1}}=1,[a_1,a_2]=a_3^{p^{m_3}},[a_1,a_3]=a_2^{p^{m_2}},[a_2,a_3]=1\rangle$, $m_1\geqslant m_2=m_3+1$. A 是满足 $\exp(A)\leqslant p^{m_3}$ 的交换群;

(2) $G=K\times A$. 其中 $K=\langle a_1,a_2,a_3 \mid a_1^{p^{m_1}}=a_2^{p^{m_2+1}}=a_3^{p^{m_3+1}}=1,[a_1,a_2]=a_3^{p^{m_3}},[a_1,a_3]=a_2^{\nu p^{m_2}},[a_2,a_3]=1\rangle$. 其中 p 为奇素数, ν 是一个固定的模 p 的平方非剩余, $m_1\geqslant m_2=m_3+1$ 或者 $m_1\geqslant m_2=m_3$, A 是满足 $\exp(A)\leqslant p^{m_3}$ 的交换群;

(3) $G=K\times A$. 其中 $K=\langle a_1,a_2,a_3 \mid a_1^{p^{m_1}}=a_2^{p^{m_2+1}}=a_3^{p^{m_3+1}}=1,[a_1,a_2]=a_3^{p^{m_3}},[a_1,a_3]=a_2^{kp^{m_2}}a_3^{-p^{m_3}},[a_2,a_3]=1\rangle$. 其中 $m_1\geqslant m_2=m_3$. 若 p 为奇素数, 则 $1+4k$ 是模 p 的平方非剩余; 若 $p=2$, 则 $k=1$. A 是满足 $\exp(A)\leqslant p^{m_3}$ 的交换群;

(4) $G=K\times A$. 其中 $K=\langle a_1,a_2,a_3 \mid a_1^{p^{m_1+1}}=a_2^{p^{m_2+1}}=a_3^{p^{m_3}}=1,[a_1,a_2]=a_1^{p^{m_1}},[a_1,a_3]=a_2^{p^{m_2}},[a_2,a_3]=1\rangle$, 其中 $m_1\geqslant m_2\geqslant m_3$. A 是满足 $\exp(A)\leqslant p^{m_2}$ 的交换群;

(5) $G=K\times A$. 其中 $K=\langle a_1,a_2,a_3 \mid a_1^{p^{m_1+1}}=a_2^{p^{m_2}}=a_3^{p^{m_3+1}}=1,[a_1,a_2]=a_3^{p^{m_3}},[a_1,a_3]=a_1^{p^{m_1}},[a_2,a_3]=1\rangle$. 其中 $m_1\geqslant m_2=m_3+1$. A 是满足 $\exp(A)\leqslant p^{m_3}$ 的交换群;

(6) $G=K\times A$. 其中 $K=\langle a_1,a_2,a_3 \mid a_1^{p^{m_1+1}}=a_2^{p^{m_2+1}}=a_3^{p^{m_3}}=1,[a_1,a_2]=1,[a_1,a_3]=a_2^{p^{m_2}},[a_2,a_3]=a_1^{p^{m_1}}\rangle$. 其中 $m_1-1=m_2\geqslant m_3$. A 是满足 $\exp(A)\leqslant p^{m_2}$ 的交换群;

(7) $G=K\times A$. 其中 $K=\langle a_1,a_2,a_3 \mid a_1^{p^{m_1+1}}=a_2^{p^{m_2+1}}=a_3^{p^{m_3}}=1,[a_1,a_2]=1,[a_1,a_3]=a_2^{p^{m_2}},[a_2,a_3]=a_1^{\nu p^{m_1}}\rangle$, 其中 p 为奇素数, ν 是一个固定的模 p 的平方非剩余, $m_1-1=m_2\geqslant m_3$ 或者 $m_1=m_2>m_3$, A 是满足 $\exp(A)\leqslant p^{m_2}$ 的交换群;

(8) $G = K \times A$. 其中 $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3}} = 1, [a_1, a_2] = 1, [a_1, a_3] = a_2^{p^{m_2}}, [a_2, a_3] = a_1^{kp^{m_1}} a_2^{-p^{m_2}} \rangle$, 其中 $m_1 = m_2 > m_3$, 若 p 为奇素数, 则 $1 + 4k$ 是模 p 的平方非剩余; 若 $p = 2$, 则 $k = 1$. A 是满足 $\exp(A) \leqslant p^{m_2}$ 的交换群;

(9) $G = K \times A$. 其中 $K = \langle a_1, a_2, b \mid a_1^4 = a_2^4 = 1, b^2 = a_1^2, [a_1, a_2] = 1, [a_1, b] = a_2^2, [a_2, b] = a_1^2 \rangle$, A 是满足 $\exp(A) \leqslant 2$ 的交换群;

(10) $G = K \times A$. 其中 $K = \langle a_1, a_2, b, d \mid a_1^4 = a_2^4 = 1, b^2 = a_1^2, d^2 = a_2^2, [a_1, a_2] = 1, [a_1, b] = a_2^2, [a_2, b] = a_1^2, [a_1, d] = a_1^2, [a_2, d] = a_1^2 a_2^2, [b, d] = 1 \rangle$, A 是满足 $\exp(A) \leqslant 2$ 的交换群.

类型 *(IV)*: $c(G) = 2$ 且 G' 为 p^3 阶初等交换群. G 有以下几种互不同构的类型:

(1a) $G = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3+1}} = 1, [a_1, a_2] = a_3^{p^{m_3}}, [a_1, a_3] = a_2^{\nu p^{m_2}}, [a_2, a_3] = a_1^{p^{m_1}} \rangle$, 其中 p 为奇素数, ν 是一个固定的模 p 的平方非剩余, $m_1 = m_2 = m_3 + 1$;

(1b) $G = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3+1}} = 1, [a_1, a_2] = a_3^{p^{m_3}}, [a_1, a_3] = a_1^{p^{m_1}} a_2^{lp^{m_2}}, [a_2, a_3] = a_1^{p^{m_1}} \rangle$, 其中 $m_1 = m_2 = m_3 + 1$. 若 $p = 2$, 则 $l = 1$; 若 $p > 2$, 则 $4l = g^{2r+1} - 1$, $r = 1, 2, \ldots, \frac{1}{2}(p-1)$, g 是模 p 的最小原根;

(2) $G = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3+1}} = 1, [a_1, a_2] = a_3^{p^{m_3}}, [a_1, a_3] = a_2^{\nu p^{m_2}}, [a_2, a_3] = a_1^{p^{m_1}} \rangle$. 其中 p 为奇素数, ν 是一个固定的模 p 的平方非剩余, $m_1 = m_2 + 1 = m_3 + 1$;

(3) $G = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3+1}} = 1, [a_1, a_2] = a_3^{p^{m_3}}, [a_1, a_3] = a_2^{kp^{m_2}} a_3^{-p^{m_3}}, [a_2, a_3] = a_1^{p^{m_1+1}} \rangle$. 其中 $m_1 = m_2 + 1 = m_3 + 1$, 若 p 为奇素数, 则 $1 + 4k$ 是模 p 的平方非剩余; 若 $p = 2$, 则 $k = 1$;

(4) $G = \langle a_1, a_2, a_3 \mid a_1^4 = a_2^4 = a_3^4 = 1, [a_1, a_2] = a_3^2, [a_1, a_3] = a_2^2 a_3^2, [a_2, a_3] = a_1^2 a_2^2 \rangle$.

类型 *(V)*: 亚循环的亚 *Hamilton* p 群. G 有以下几种互不同构的类型:

(1) $G = \langle a, b \mid a^{p^{r+s+u}} = 1, b^{p^{r+s+t}} = a^{p^{r+s}}, a^b = a^{1+p^r} \rangle$. 其中 $r \geqslant 1$, $u \leqslant r$ 和 $r + 1 \geqslant s + u \geqslant 2$. 并且若 $p = 2$, 则 $r \geqslant 2$;

(2) $G = \langle a, b \mid a^{2^3} = b^{2^m} = 1, a^b = a^{-1} \rangle$;

(3) $G = \langle a, b \mid a^{2^3} = 1, b^{2^m} = a^4, a^b = a^{-1} \rangle$;

(4) $G = \langle a, b \mid a^{2^3} = b^{2^m} = 1, a^b = a^3 \rangle$.

类型 (VI): G' 循环的非亚循环的亚 Hamilton p 群, 此时一定有 $d(G) \geqslant 3$. G 有以下几种互不同构的类型:

(1) $G = K \times A$. 其中 $K = \langle a, b \mid a^{p^{r+s+u}} = 1, b^{p^{r+s}} = 1, a^b = a^{1+p^r} \rangle$, $u \leqslant r$, $r + 1 > s + u \geqslant 2$, A 是满足 $\exp(A) \leqslant p^{(r+1)-(s+u)}$ 的非平凡的交换群;

(2) $G = K \times A$. 其中 $K = \langle a, b \mid a^{p^{r+t+u}} = 1, b^{p^r} = 1, a^b = a^{1+p^{r+t}} \rangle$, $t \geqslant 1$, $r \geqslant u \geqslant 2$. A 是满足 $\exp(A) \leqslant p^{t+(r+1)-u}$ 的非平凡的交换群;

(3) $G = K \times A$. 其中 $K = \langle a, b \mid a^{p^{r+s}} = 1, b^{p^{r+s+t}} = 1, a^b = a^{1+p^r} \rangle$, $t \geqslant 1$, $r + 1 > s \geqslant 2$, A 是满足 $\exp(A) \leqslant p^{(r+1)-s}$ 的非平凡交换群;

(4) $G = K \times A$. 其中 $K = \langle a, b \mid a^{p^{r+s+u}} = 1, b^{p^{r+s+t}} = a^{p^{r+s}}, a^b = a^{1+p^r} \rangle$, $stu \neq 0$, $r+1 > s+u \geqslant 2$, A 是满足 $\exp(A) \leqslant p^{(r+1)-(s+u)}$ 的非平凡交换群;

(5) $G = (K \rtimes B) \times A$. 其中 $K = \langle a, b \mid a^{p^{r+t+u}} = 1, b^{p^r} = 1, a^b = a^{1+p^{r+t}} \rangle$. $B = \langle b_1 \rangle \times \langle b_2 \rangle \times \cdots \times \langle b_f \rangle$ 满足 $o(b_i) = p^{r_i}$, $[a, b_i] = a^{p^{r+t_i}}$, $[b, b_i] = 1$, $\max\{t, u-2\} < t_1 < t_2 < \cdots < t_f < t + u$, $r + t > r_1 + t_1 > r_2 + t_2 > \cdots > r_f + t_f \geqslant t + u \geqslant t + 2$. A 是满足 $\exp(A) \leqslant p^{t+(r+1)-u}$ 的交换群.

类型 (VII): G' 的型不变量为 (p^α, p)(其中 $\alpha \geqslant 2$) 的亚 Hamilton p 群. G 有以下几种互不同构的类型:

(1) $G = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1+m_2}} = a_2^{p^{m_2+1}} = a_3^p = 1, [a_1, a_2] = a_1^{p^{m_1}}, [a_1, a_3] = a_2^{p^{m_2}}, [a_2, a_3] = 1 \rangle$, 其中 $m_1 > m_2 \geqslant 1$, p 为奇素数;

(2) $G = K \times A$. 其中 $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1+k}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3}} = 1, [a_1, a_2] = a_1^{p^{m_1}}, [a_1, a_3] = a_2^{p^{m_2}}, [a_2, a_3] = 1 \rangle$, $m_1 \geqslant m_2 \geqslant m_3$, $1 \leqslant k \leqslant \min\{m_1 - m_3, m_2 - m_3 + 1, m_2 - 1\}$. A 是满足 $\exp(A) \leqslant p^{m_2 - k}$ 的交换群.

参考文献

[1] 陈重穆. 内外 Σ 群与极小非 Σ 群. 重庆: 西南师范大学出版社, 1988.

[2] 吕恒、陈贵云, 一类特殊的有限 p 群, 东北师大学报（自然科学版）, **39**(2007), 19–21.

[3] 宋蔷薇、曲海鹏, 所有子群皆循环或正规的有限 2 群, 数学的实践与认识, **10**(2008), 191–197.

[4] 徐明曜, 奇阶亚循环 p 群的完全分类, 数学进展, **12**(1983), 72–73.

[5] 徐明曜. 有限群导引（上册）, 北京: 科学出版社, 1987. 第 2 版, 1999.

[6] 徐明曜、曲海鹏, 有限 p 群, 北京: 北京大学出版社, 2010.

[7] 徐明曜、黄建华、李慧陵、李世荣, 有限群导引（下册）, 北京: 科学出版社, 2001.

[8] An L J, Qu H P, Xu, M Y, Yang C S. Quasi-NC groups. Comm. Algebra, 2008, 36(11): 4011–4019.

[9] An L J, Li L L, Qu H.P, Zhang Q H. Finite p-groups with a minimal non-abelian subgroup of index p (II). Sci. China Math., 2014, 57(4): 737-753.

[10] An L J. Hu R F, Zhang Q H. Finite p-groups with a minimal nonabelian subgroup of index p (IV). J. Algebra Appl., 2015, 14(2) 155020.

[11] An L J, Ding J F, Zhang Q H. Finite self dual groups. J. Algebra, 2011, 341: 35–44.

[12] An L J, Peng J. Finite p-groups in which any two noncommutative elements generate an inner abelian group of order p^4. Algebra Colloq., 2013, 20(2): 215-226.

[13] An L J, Brennan J, Qu H P, Wilcox E. Chermak-Delgado lattice extension theorems. Comm. Algebra, 2015, 43(5): 2201-2213.

[14] An L J, Zhang Q H. Finite metahamiltonian p-groups. (2015) J. Algebra, http://dx.doi.org/10.1016/j.jalgebra.2014.12.004.

[15] R. Baer, Situation der Untergruppen und struktur der Gruppen, *S. B. Heidelberg Akad. Mat. Nat.*, **2**(1933), 12–17.

[16] Y. Berkovich and Z. Janko. Structure of finite p-groups with given subgroups, *Contemporary Math.*, **402**(2006), 13–93.

[17] Y. Berkovich and Z. Janko, *Groups of Prime Power Order, volume 2*, Walter de Gruyter, Berlin, 2008.

[18] N.Blackburn, Generalizations of certain elementary theorems on p-groups, *Proc. London Math. Soc.* (3)**11**(1961), 1-22.

[19] N. Blackburn, On a special class of p-groups, *Acta Math.* **100**(1958), 45-92.

[20] S.R. Balckburn, Enumeration within isoclinism classes of groups of prime order, *J. London Math. Soc.,* (2) **50**(1994), no. 2, 293-304.

[21] R. Dedekind, Über Gruppen, deren samtliche Teiler Normalteiler sind, *Math. Ann.*, **48**(1897), 548–561.

[22] S. V. Draganyuk, On the structure of finite primary groups all 2-maximal subgroups of which are abelian (Russian), *Complex analysis, Algebra and topology, Akad. Nauk Ukrain. SSR, Inst. Mat., Kiev.*(1990), 42–51.

[23] G. Glauberman, Large subgroups of small class in finite p-groups, *J. Algebra*, **272**(2004), 128–153.

[24] G. Glauberman, Abelian subgroups of small index in finite p-groups, *J. Group Theory*, **8**(2005), 539–560.

[25] G. Glauberman, Centrally large subgroups of finite p-groups, *J. Algebra*, **300**(2006), 480–508.

[26] D. Gorenstein, R. Lyons, and R. M. Solomon, *The Classification of the Finite Simple Groups, Number 1*, Amer. Math. Soc. Surveys and Monographs **40, #1** (1995).

[27] D. Gorenstein, R. Lyons, and R. M. Solomon, *The Classification of the Finite Simple Groups, Number 2*, Amer. Math. Soc. Surveys and Monographs **40, #2** (1996).

[28] D. Gorenstein, R. Lyons, and R. M. Solomon, *The Classification of the Finite Simple Groups, Number 3*, Amer. Math. Soc. Surveys and Monographs **40, #3** (1998).

[29] D. Gorenstein, R. Lyons, and R. M. Solomon, *The Classification of the Finite Simple Groups, Number 4*, Amer. Math. Soc. Surveys and Monographs **40, #4** (1999).

[30] D. Gorenstein, R. Lyons, and R. M. Solomon, *The Classification of the Finite Simple Groups, Number 5*, Amer. Math. Soc. Surveys and Monographs **40, #5** (2002).

[31] D. Gorenstein, R. Lyons, and R. M. Solomon, *The Classification of the Finite Simple Groups, Number 6*, Amer. Math. Soc. Surveys and Monographs **40, #6** (2005).

[32] L. S. Kazarin, On certain classes of finite groups, *Dokl. Akad. Nauk SSSR (Russian)*, **197**(1971), 773–776.

[33] M. Hall, *The Theory of Groups*, Macmillan Company, New York (1959).

[34] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, 1967.

[35] Z. Janko, Finite 2-groups with small centralizer of an involution, *J. Algebra*, **241**(2001), no. 2, 818–826.

[36] Z. Janko, Finite 2-groups with small centralizer of an involution. II, *J. Algebra*, **245**(2001), no. 1, 413–429.

[37] Z. Janko, Finite 2-groups with no normal elementary abelian subgroup of order 8, *J. Algebra*, **246**(2001), 951–961.

[38] Z. Janko, Finite 2-groups with a self-centralizing elementary abelian subgroup of order 8, *J. Algebra*, **269**(2003), 189–214.

[39] Z. Janko, Elements of order at most 4 in finite 2-groups, *J. Group Theory*, **7**(2004), 431–436.

[40] Z. Janko, 2-groups with a self-centralizing abelian subgroup of type (4,2), *Glas. Mat. Ser.*, III **39**(59)(2004), no. 2, 235–243.

[41] Z. Janko, A classification of finite 2-groups with exactly three involutions, *J. Algebra*, **291**(2005), no. 2, 505–533.

[42] Z. Janko, Finite 2-groups all of whose maximal cyclic subgroups of composite order are self-centralizing, *J. Group Theory*, **10**(2007), no. 1, 1–4.

[43] B. W. King, Presentations of metacyclic groups, *Bull. Aus. Math. Soc.*, **8**(1973), 101–131.

[44] N. F. Kuzennyi and N. N. Semko, *Structure of periodic met-Abelian meta-Hamiltonian groups with nonelementary commutant*, Ukr. Mat. Zh. **39**, (1987) No.2, 180-185.

[45] N. F. Kuzennyi and N. N. Semko, *Meta-hamiltonian groups with elementary commutant of rank 2*, Ukr. Mat. Zh. **42**, (1990) No.2, 168-175.

[46] V. T. Nagrebeckii, Invariant coverings of subgroups, *Ural Gos. Univ. Mat. Zap.*, **5**(1966), 91–100.

[47] V. T. Nagrebeckii, Finite non-nilpotent groups, any non-abelian subgroup of which is normal, *Ural Gos. Univ. Mat. Zap.*, **6**(1967), 80–88.

[48] V. T. Nagrebeckii, Finite groups in which any non-nilpotent subgroups is invariant, *Ural Gos. Univ. Mat. Zap.*, **7** (1968), 45–49.

[49] M. F. Newman, Determination of groups of prime-power order, *Group theory, (Caberra 1975)*, Lecture Notes in Math., **573**(1977), 73–84.

[50] M. F. Newman and Ming-Yao Xu, Metacyclic groups of prime-power order, (preprint), 1987.

[51] M. F. Newman and Ming-Yao Xu, Metacyclic groups of prime-power order (Research announcement), *Adv. in Math. (China)*, **17**(1988), 106–107.

[52] D. S. Passman, Nonnormal subgroups of p-groups, *J. Algebra*, **15**(1970), 352–370.

[53] G. L. Peterson, Finite metacyclic I-E and I-A groups, *Comm. Algebra*, **23**(1995), 4563–4585.

[54] L.*Rédei*, Das schiefe Product in der Gruppentheorie, *Comment.Math.Helvet.*, **20**(1947), 225–267.

[55] G. M. Romalis and N. F. Sesekin, Metahamiltonian groups, *Ural. Gos. Univ. Mat. Zap.*, **5**(1966), 101–106.

[56] G. M. Romalis and N. F. Sesekin, Metahamiltonian groups II, *Ural. Gos. Univ. Mat. Zap.*, **6**(1968), 52–58.

[57] G. M. Romalis and N. F. Sesekin, Metahamiltonian groups III, *Ural. Gos. Univ. Mat. Zap.*, **7**(1969–1970), 195–199.

[58] V. A. Sheriev, A description of the class of finite p-groups whose 2-maximal subgroups are all abelian II, in Primary groups, *Proc. Sem. Algebraic Systems*, **2**(1970), 54–76.

[59] G. Silberberg, Finite equilibrated 2-generated 2-groups, *Acta Math. Hungar.*, **110**(2006), 23–35.

[60] H.F. Tuan (1948), An Anzahl theorem of Kulakoff's type for p-groups, *Sci. Rep. Nat. Tsing-Hua Univ. Ser. A*, **5**, 182–189. MR0030948 (11,77e)

[61] Ming-Yao Xu, Three presentations for metacyclic 2-groups, (Appendix to "Metacyclic groups of prime-power order"), preprint, 1987.

[62] Mingyao Xu and Qinhai Zhang, A Classification of Metacyclic 2-Groups, *Alg. Colloq.*, **13**(2006), 25–34.

[63] Qinhai Zhang, Xiujuan Sun, Lijian An and Mingyao Xu, Finite p-groups all of whose subgroups of index p^2 are abelian, *Algebra Colloq.*, **15:1**(2008), 167–180.

[64] Qinhai Zhang, Xiaoqiang Guo, Haipeng Qu and Mingyao Xu, Finite groups which have many normal subgroups, *J. Korean Math. Soc.*, **46**(2009), 1165-1178.